KASPERSKY LAB

Kaspersky® Anti-Virus para Windows Workstations 6.0

MANUAL DE UTILIZADOR

KASPERSKY® ANTI-VIRUS PARA WINDOWS WORKSTATIONS 6.0

Manual de utilizador

http://www.kaspersky.com

Data de Revisão: Julho de 2007

Índice

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DO COMPUTADOR

O número de crimes destinados a quebrar a segurança da informação cresceu, dado que as tecnologias de informação desenvolveram-se rapidamente e penetraram em todos os aspectos da existência humana.

Os criminosos do ciberespaço demonstraram grande interesse na actividade das estruturas estatais e dos empreendimentos comerciais. Fazem tentativas de roubo e divulgação de informação confidencial, destruindo reputações de empresas, quebrando a continuidade de negócios e danificando, por consequência, os recursos informativos de uma organização. Estes actos podem causar danos extensivos a bens, tanto tangíveis, como intangíveis.

Não são apenas as grandes companhias que correm riscos. Os utilizadores individuais também podem ser atacados. Usando várias ferramentas, os criminosos ganham acesso a dados pessoais (contas bancárias, números de cartões de crédito e passwords), provocam avarias no seu sistema ou obtêm acesso completo ao computador.

No mundo de hoje, todos reconhecem que a informação é um bem valioso e que deverá ser protegido. Ao mesmo tempo, a informação deve estar acessível a um determinado grupo de utilizadores (por exemplo, empregados, clientes e parceiros de um negócio). Esta é a razão porque há uma necessidade de criar um sistema de segurança de informação global. Este sistema deverá tomar em conta todas as possíveis fontes de ameaças, quer sejam humanas, feitas pelo Homem, ou acidente naturais, e usar uma série completa de medidas defensivas, a nível físico, administrativo e de software.

1.1. Fontes de ameaças

Uma pessoa, um grupo de pessoas, ou mesmo alguns fenómenos não relacionados com a actividade humana, poderão servir como uma ameaça à segurança de informação. Deste modo, todas as fontes de ameaças dividem-se em três grupos:

- **O factor humano**. Este grupo de ameaças diz respeito às acções de pessoas com acesso autorizado ou não-autorizado à informação. As ameaças neste grupo podem ser divididas em:

- *Externas*, incluindo criminosos do ciberespaço, hackers, fraudes na Internet, sócios pouco escrupulosos e estruturas criminais.
   - *Internas*, incluindo acções de empregados da empresa e utilizadores de computadores pessoais domésticos. As acções tomadas por este grupo podem ser deliberadas ou acidentais.
- **O factor tecnológico**. Este grupo de ameaças está ligado a problemas técnicos – equipamento usado que se tornou obsoleto e a má qualidade de software e hardware de processamento de informação. Tudo isto leva a avarias de equipamento e a perdas frequentes de dados.
- **O factor do desastre natural**. Este grupo de ameaça inclui qualquer número de ocorrências levadas a cabo pela Natureza e outras ocorrências independentes da actividade humana.

Todas as três fontes de ameaças devem ser tomadas em conta quando se desenvolver um sistema de segurança de protecção de dados. Este manual de utilizador apenas cobre o que está directamente ligado à experiência da Kaspersky Lab – ameaças externas envolvendo actividade humana.

1.2. Como se espalham as ameaças

À medida que a moderna tecnologia de computadores e ferramentas de comunicação se desenvolvem, os hackers têm mais oportunidades para espalhar ameaças. Vejamo-las mais de perto:

A Internet

A Internet é única, dado que não é propriedade de ninguém e não tem limites geográficos. Promoveu de vários modos o desenvolvimento de inúmeros recursos da Internet e a troca de informação. Hoje, qualquer um pode aceder a dados na Internet ou criar a sua própria página Web.

Contudo, estas mesmas funções da Web mundial dão aos hackers a capacidade para cometer crimes na Internet, tornando-os difíceis de detectar e punir enquanto são efectuados.

Os hackers colocam vírus e outros programas maliciosos em páginas de Internet e disfarçam-nas como utilitários úteis gratuitos. Adicionalmente, scripts que sejam automaticamente executados quando abre determinadas páginas de Internet podem agir perigosamente no seu computador, incluindo a modificação do registo do sistema, o roubo de dados pessoais e instalação de software malicioso.

Ao utilizar tecnologias de rede, os hackers podem atacar PCs remotos e servidores de empresas. Estes ataques podem levar a que partes do seu sistema funcionem mal ou podem dar aos hackers um acesso completo ao seu sistema e à informação guardada nele. Também podem usá-lo como parte de uma rede zombie.

Desde que se tornou possível usar cartões de crédito e dinheiro electrónico através da Internet em lojas online, leilões e páginas de bancos, as fraudes online surgiram como um dos crimes mais comuns.

Intranet

A intranet é a rede interna, concebida especificamente para tratar de informação no seio da empresa ou numa rede doméstica. Uma intranet é um espaço unificado para guardar, trocar e aceder à informação em todos os computadores da rede. Isto significa que, se um dos computadores da rede estiver infectado, os outros correm um grande risco de infecção. Para evitar essas situações, quer o perímetro da rede, quer cada computador individual devem estar protegidos.

E-mail

Dado que, praticamente, todos os computadores têm clientes de e-mail instalados e visto que programas maliciosos exploram o conteúdo das agendas electrónicas, existem condições apropriadas para espalhar programas maliciosos. O utilizador de um computador infectado, estando alheado do facto, pode enviar e-mails infectados a amigos ou colegas, que por sua vez enviam mais e-mails infectados. É habitual que documentos infectados fiquem indetectados e sejam enviados com informação de negócios de uma grande empresa. Quando isto acontece, mais do que um punhado de pessoas são infectadas. Podem ser centenas ou milhares, todas a enviar ficheiros infectados a dezenas de milhares de assinantes.

Para além da ameaça de programas maliciosos. existe o programa de correio electrónico de lixo ou spam. Apesar de não ser uma ameaça directa ao seu computador, o spam aumenta a carga nos servidores de correio, consome largura de banda, enche a sua caixa de correio e implica o desperdício de muitas horas de trabalho, causando por isso problemas financeiros.

Além disto, note que os hackers começaram a usar programas de correio em massa e métodos de engenharia social para convencer os utilizadores a abrir e-mails ou a clicar numa hiperligação para certas páginas de Internet. Portanto, as capacidades de filtragem de spam são importantes, tanto para deter o lixo electrónico, como também para se contrapor a novos tipos de verificação online, como o “phishing”, e para impedir a distribuição de programas maliciosos.

Meios amovíveis de armazenamento

Meios amovíveis (disquetes, CD/DVD-ROMs e unidades de armazenamento USB) são amplamente usadas para guardar e transmitir informação.

Ao abrir um ficheiro com código malicioso, a partir de um meio amovível de armazenamento, poderá danificar dados guardados no computador e espalhar vírus pelas outras unidades do computador ou outros computadores da rede.

1.3. Tipos de Ameaças

Existe um grande número de ameaças que podem afectar hoje o computador. Esta secção abordará as ameaças que o Kaspersky Anti-virus para Windows Workstations.

Vermes (Worms)

Esta categoria de programa malicioso explora, amplamente, as vulnerabilidades do sistema operativo para se espalhar. A classe foi designada devido ao modo como os worms (vermes) passam de computador para computador, usando redes e e-mails. Esta capacidade dá aos worms uma maior velocidade para se espalharem.

Quando um worm penetra num computador, este procura os endereços de rede de outros computadores localmente acessíveis e envia uma quantidade de cópias por si executadas para esses endereços. Para além disso, os worms utilizam com frequência dados de agendas de endereços de clientes de e-mail. Alguns destes programas maliciosos criam por vezes ficheiros de trabalho em discos de sistema, mas podem ser executados sem quaisquer recursos de sistema (com excepção da memória RAM).

Vírus

Programas que infectaram outros programas, juntando-lhes o seu próprio código para ganhar controlo de ficheiros infectados quando estes são abertos. Esta definição simples explica a acção fundamental executada por um vírus – *infecção*.

Cavalos de Tróia (Trojans)

Programas que executam acções não autorizadas em computadores, como, por exemplo, apagar informação em unidades, provocando o bloqueio do sistema, roubar informação confidencial, etc. Esta classe de programas maliciosos não é um vírus no sentido tradicional do termo (significando que não infecta outros computadores ou dados). Os cavalos de Tróia (Trojans) não podem entrar em computadores por si só. São espalhados por hackers,

que os disfarçam de software comum. Os danos que podem trazer podem exceder várias vezes os ataques de vírus tradicionais.

Recentemente, os worms têm sido o tipo de programa malicioso mais espalhado para danificar dados de computadores. Depois seguem-se os vírus e cavalos de Tróia. Alguns programas maliciosos combinam funções de dois ou mesmo três destas classes.

Software com publicidade (Adware)

Código de programa incluído no software, desconhecido para o utilizador, concebido para mostrar anúncios. O adware está habitualmente incorporado no software de livre distribuição. A publicidade está situada na interface do programa. Estes programas reúnem com frequência dados pessoais do utilizador e enviam-nos para o programador, alteram as definições do navegador (páginas de abertura e de pesquisa, níveis de segurança, etc.) e criam tráfego que o utilizador não pode controlar. Tudo isto pode levar à quebra da política de segurança e a perdas financeiras directas.

Software espião (Spyware)

Software que recolhe informação sobre um utilizador em particular ou organização sem o seu conhecimento. Poderá nunca saber que tem spyware instalado no seu computador. Em geral, o objectivo do spyware é:

- Registar as acções do utilizador num computador;
- Reunir informação sobre o conteúdo do seu disco rígido; nestes casos, envolve a busca de alguns directórios e o registo do sistema para compilar uma lista do software instalado no computador;
- Reunir informação sobre a qualidade da ligação de rede, a largura de banda, a velocidade do modem, etc.

Software potencialmente perigoso (Riskware)

O riskware inclui software que não tem funções maliciosas, mas pode fazer parte do ambiente de desenvolvimento para programas maliciosos ou que pode ser usado por hackers como componentes auxiliares para programas maliciosos. Esta categoria de programas inclui programas com portas de comunicação escondidas e vulnerabilidades, assim como algumas utilidades para administração remota, programas de alternância automática da disposição do teclado, clientes de IRC, servidores FTP e utilitários gerais para parar processos ou esconder o seu funcionamento.

Outro tipo de programa malicioso, que acompanha programas como adware, spyware e riskware, são os programas que se instalam no navegador da Web e redireccionam o tráfego. Certamente, já deve ter encontrado estes programas se tiver aberto uma página da Web quando pensava que estava abrir outra.

Programas de brincadeiras (Jokes)

Software que não tenta fazer qualquer dano directo, mas exibe mensagens que afirmam já terem sido causados danos ou que serão causados danos em certas condições. Estes programas, frequentemente, avisam o utilizador de perigos que não existem, como as mensagens que surgem sobre a formatação do disco rígido (apesar de nenhuma formatação ter sido feita, na realidade), ou detectam vírus em ficheiros não infectados.

Processos ocultos (Rootkits)

Utilitários usados para esconder actividades maliciosas. Camuflam-se em programas maliciosos para evitarem que os programas anti-vírus os detectem. Os rootkits modificam o sistema operativo do computador e alteram as suas funções básicas, para esconder a sua própria existência e acções que o hacker executa no computador infectado.

Outros programas perigosos

Programas criados para activar ataques DoS (recusa de serviço) em servidores remotos, penetrando noutros computadores, e ainda programas que são parte do ambiente de desenvolvimento de programas maliciosos. Estes programas incluem ferramentas de penetração, desenvolvimento de vírus, de procura de vulnerabilidades, programas para descobrir passwords e outros tipos de programas para descobrir recursos de rede ou penetrar num sistema.

Ataques de hackers

Os ataques de hackers podem ser iniciados por eles ou por programas maliciosos. São destinados a roubar informação de um computador remoto, provocando uma avaria do sistema ou obtendo controlo total dos recursos do sistema. Na secção 12.9, na pág. 171, pode encontrar uma descrição detalhada dos tipos de ataque que o Kaspersky Anti-virus para Windows Workstations bloqueia.

Alguns tipos de fraude online

Phishing é uma fraude online que usa o envio em massa de e-mails no sentido de roubar informação confidencial do utilizador, geralmente de natureza financeira. Os e-mails de phishing são feitos para se parecerem, o mais possível, com e-mails informativos de bancos e empresas conhecidas. Estes e-mails contêm hiperligações para páginas falsas, elaboradas por hackers para copiar o site da organização que pretendem representar. Neste site, pede-se ao utilizador para introduzir, por exemplo, o número do cartão de crédito e outra informação confidencial.

Programas de marcação telefónica para páginas de Internet pagas – um tipo de fraude online que utiliza serviços de Internet pagos não-autorizados (estes são habitualmente páginas Web de natureza

pornográfica). Os programas de marcação telefónica, instalados por hackers, inicializam ligações de modem a partir do computador para o número do serviço pago. Estes números têm, frequentemente, preços altos e o utilizador é obrigado a pagar contas enormes de telefone.

Publicidade intrusiva

Esta inclui janelas e faixas de anúncios que se abrem quando usa o navegador de Internet. A informação nestas janelas é, geralmente, de nenhum benefício para si. Janelas que se abrem e faixas de publicidade distraem o utilizador da tarefa e consomem largura de banda.

Spam

O Spam consiste em correio electrónico não-solicitado anónimo. O spam inclui mailings de marketing, de natureza política e provocante e e-mails a pedir assistência. Outra categoria de spam inclui e-mails que pedem a alguém para investir grandes quantidades de dinheiro ou para se envolver em esquemas de pirâmide, e-mails destinados a roubar passwords e números de cartões de crédito e e-mails que pedem para serem enviados a amigos (cartas circulares).

O Spam aumenta, significativamente, a carga nos servidores de e-mail e o risco de perder dados importantes.

O Kaspersky Anti-Virus para Windows Workstations usa dois métodos para detectar e bloquear estes tipos de ameaça:

- *Reactivos* – este método procura ficheiros maliciosos, usando uma base de dados de assinaturas de ameaças que é actualizada regularmente. É necessária pelo menos uma infecção de vírus para implementar este método - por forma a adicionar assinaturas de ameaças à base de dados e distribuir actualizações da base de dados.
- *Proactivos* – em contraste com a protecção reactiva, este método não se baseia na análise de código dos objectos, mas sim na análise do seu comportamento no sistema. Este método destina-se a detectar novas ameaças que ainda não estão definidas nas assinaturas.

Ao empregar ambos os métodos, o Kaspersky Anti-virus para Windows Workstations permite uma protecção abrangente do computador em relação a ameaças conhecidas e novas.

Aviso:

A partir daqui, usaremos o termo "vírus" para nos referirmos a programas maliciosos e perigosos. O tipo de programas maliciosos apenas serão enfatizados quando necessário.

1.4. Sinais de Infecção

Existe um certo número de sinais quando o computador está infectado. Se notar que o computador está a fazer coisas estranhas, especificamente:

- Mensagens inesperadas ou imagens que aparecem no ecrã ou são emitidos sinais inabituais;
- A gaveta do CD/DVD-ROM abre-se e fecha-se inesperadamente;
- O computador abre ao acaso um programa sem a sua assistência;
- Surgem avisos no ecrã sobre um programa do seu computador que tenta aceder à Internet, mesmo que não tenha iniciado essa acção;

Também há vários sinais típicos de uma infecção por vírus através do e-mail:

- Amigos ou conhecidos falam-lhe de mensagens que nunca enviou;
- A sua caixa de correio contém um grande número de mensagens sem remetente ou cabeçalhos.

É de notar que estes sinais podem resultar de problemas diferentes de vírus. Por vezes, podem surgir por causas variadas. Por exemplo, no caso de e-mails, podem ser enviadas mensagens infectadas com o seu endereço de retorno mas que não foram enviadas a partir do seu computador.

Também há indicações indirectas de infecção do seu computador:

- O computador bloqueia ou fica parado com frequência;
- O computador carrega programas lentamente;
- Não consegue carregar o sistema operativo;
- Ficheiros e pastas desaparecem ou o seu conteúdo é distorcido;
- O disco rígido é frequentemente acedido (a luz pisca);
- O navegador da Internet (por exemplo, o Microsoft Internet Explorer) bloqueia ou comporta-se de modo inesperado (por exemplo, não consegue fechar a janela de programas).

Em 90% dos casos, estes sistemas indirectos são provocados por avarias no hardware ou software. Apesar do facto de esses sintomas raramente indicarem que o computador esteja infectado, recomendamos que, ao detectá-los, faça uma verificação completa no computador (ver 5.2 na pág. 65).

1.5. O que fazer se houver sinais de infecção

Se notar que o seu computador se comporta de modo suspeito…

1. Não entre em pânico! Não ceda ao pânico. Esta é a regra dourada e pode poupar-lhe dados importantes.
2. Desligue o computador da Internet ou rede local, se estiver ligado a uma.
3. Se o sintoma de infecção for o de não poder arrancar a partir do disco rígido do computador (o computador exibe uma mensagem de erro quando o liga), experimente arrancar em modo de segurança ou com o disco de emergência do Windows que criou quando instalou o sistema operativo no computador.
4. Antes de fazer mais alguma coisa, faça uma cópia de segurança do seu trabalho para meios amovíveis de armazenamento (disquete, CD/DVD, unidade flash, etc.).
5. Instale o Kaspersky Anti-virus para Windows Workstations, se não o tiver já feito.
6. Actualize as assinaturas de ameaças do programa e módulos da aplicação (ver 5.6 na pág. 69). Se for possível, obtenha as actualizações da Internet a partir de um computador não infectado em casa de um amigo, num cibercafé ou no trabalho. É melhor usar um computador diferente, uma vez que quando se liga à Internet com um computador infectado, há a possibilidade de o vírus enviar informação importante a hackers ou espalhar o vírus para endereços da agenda. É por isso que, se suspeitar ter um vírus, o melhor que pode fazer é desligar-se imediatamente da Internet. Pode também obter actualizações de assinaturas de ameaças por disquete junto da Kaspersky Labs ou dos seus distribuidores e actualizar as suas assinaturas com a disquete.
7. Seleccione o nível de segurança recomendado pelos especialistas da Kaspersky Labs.
8. Inicie uma verificação completa no computador (ver 5.2 na pág. 65).

1.6. Prevenir a infecção

As medidas mais fiáveis e pensadas não podem garantir-lhe uma protecção a 100% em relação a vírus e cavalos de Tróia, mas tendo este conjunto de regras em mente, irá baixar, significativamente, a probabilidade de ataques de vírus e o nível de danos potenciais.

Um dos métodos básicos para combater os vírus é, como na medicina, a *prevenção* atempada. A profilaxia do computador envolve um número bastante reduzido de regras que, se forem obedecidas, podem baixar, significativamente, a probabilidade de ser infectado com um vírus e perder dados.

As regras básicas de segurança são apresentadas abaixo. Ao segui-las poderá evitar ataques de vírus.

Regra Nº. 1: *Use software anti-vírus e programas de segurança da Internet*. Para o fazer:

- Instale o Kaspersky Anti-virus para Windows Workstations assim que possível.
- Actualize regularmente as assinaturas de ameaças do programa (ver 5.6 na pág. 69). Pode actualizar as assinaturas várias vezes por dia durante ataques de vírus. Nestas situações, as assinaturas de ameaças nos servidores de actualização da Kaspersky Lab são imediatamente actualizadas.
- Seleccione as definições de segurança recomendadas pela Kaspersky Lab para o computador. Ficará constantemente protegido desde a altura em que o computador é ligado e será mais difícil para os vírus entrarem no seu computador.
- Configure as definições para uma verificação completa recomendada pelos especialistas da Kaspersky Lab e programe verificações, pelo menos, para uma vez por semana. Se não tiver instalado o Anti-Hacker, recomendamos que o faça para proteger o computador quando usar a Internet.

Regra Nº. 2: *Use precaução quando copiar dados novos para o computador*:

- Verifique a existência de vírus em todas as unidades amovíveis de armazenamento (disquetes, CD/DVDs, unidades flash, etc.) antes de as usar (ver 5.4 na pág. 67).
- Manuseie e-mails com cuidado. Não abra quaisquer ficheiros que tenham chegado por e-mail se não tiver a certeza de que tenham sido enviados para si, mesmo que tenham sido enviados por pessoas que conhece.

- Tenha cuidado com a informação obtida através da Internet. Se qualquer página da Internet lhe sugerir que instale um programa novo, tenha a certeza de que tem um certificado de segurança.

- Se estiver a copiar um ficheiro executável da Internet ou rede local, certifique-se de que verificou a existência de vírus com o Kaspersky Anti-virus para Windows Workstations.

- Seja criterioso ao usar as páginas de Internet que visita. Muitas páginas estão infectadas com vírus de scripts perigosos ou worms da Internet.

Regra Nº. 3: *Preste muita atenção à informação da Kaspersky Lab*.

Na maior parte dos casos, a Kaspersky Lab anuncia um novo ataque muito antes de este atingir o seu pico. A probabilidade de infecção neste caso não é tão grande e, desde que transfira as actualizações de assinaturas de ameaças, ficará com muito tempo para se proteger de novos vírus.

Regra Nº. 4: *Não confie em boatos de vírus*, tais como programas de partidas e e-mails sobre ameaças de infecção.

Regra Nº. 5: *Use a ferramenta de actualização do Windows* e instale, regularmente, as actualizações do sistema operativo Windows.

Regra Nº. 6: *Compre cópias legítimas de software nos distribuidores oficiais*.

Regra Nº. 7: *Limite o número de pessoas com permissão para usar o seu computador*.

Regra Nº. 8: *Baixe o risco de consequências desagradáveis de infecção potencial*:

- Faça cópias de segurança dos dados com regularidade. Se perder dados, o sistema pode ser restaurado com bastante rapidez se tiver as cópias de segurança. Guarde em local seguro as disquetes de distribuição, CDs, unidades flash e outros meios de armazenamento com software e informação valiosa.

- Crie um Disco de Recuperação (ver 17.10 na pág. 273) com que possa arrancar, usando um sistema operativo limpo.

Regra Nº. 9: *Inspeccione, regularmente, a lista de programas instalados no seu computador*. Para o fazer, abra a secção **Adicionar/Remover Programas** no **Painel de Controlo** ou abra o directório **Program Files**. Aqui, pode descobrir software que foi instalado no seu computador sem o seu conhecimento, por exemplo, enquanto usava a Internet ou instalava um programa. Alguns deles são quase sempre programas potencialmente perigosos.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS PARA WINDOWS WORKSTATIONS 6.0

O Kaspersky Anti-virus para Windows Workstations 6.0 é um produto da nova geração de produtos de segurança de dados.

O que distingue o Kaspersky Anti-virus para Windows Workstations 6.0 de outro software, até mesmo de outros produtos da Kaspersky Lab, é a abordagem multifacetada em relação à segurança dos dados no computador do utilizador.

2.1. O que há de novo no Kaspersky Anti-Virus para Windows Workstations 6.0

O Kaspersky Anti-Virus para Windows Workstations 6.0 constitui uma nova abordagem à segurança dados. A função principal do programa é a de combinar e melhorar, visivelmente, as funções existentes de todos os produtos da empresa através de uma solução de segurança. O programa fornece protecção contra vírus, ataques de spam, ataques de hackers, ameaças desconhecidas, phishing e rootkits.

Já não precisará de instalar vários produtos no computador para a segurança geral. Basta simplesmente instalar o Kaspersky Anti-virus para Windows Workstations 6.0.

A protecção global protege todos os canais, através dos quais entram ou são transmitidos dados. As configurações flexíveis para qualquer componente do programa dão ao Kaspersky Anti-virus para Windows Workstations a possibilidade de adaptação máxima às necessidades de cada utilizador. Também tem a opção de configurar todas as componentes de protecção a partir de um único local.

Vamos observar as novas funções do Kaspersky Anti-virus para Windows Workstations.

Novas funções de protecção

- O Kaspersky Anti-Virus para Windows Workstations protege-o não só de programas maliciosos conhecidos, como também relativamente a programas ainda desconhecidos. A defesa pró-activa (ver Capítulo 10

na pág. 127) é a principal vantagem do programa. É efectuada em torno da análise do comportamento das aplicações instaladas no computador, controlo das alterações do registo do sistema, análise de macros e combate de ameaças escondidas. A componente usa um analisador heurístico que pode detectar vários tipos de programas maliciosos. Ao fazê-lo, mantém um historial das actividades maliciosas, através do qual a actividade maliciosa pode ser revertida e o sistema pode ser reposto no seu estado anterior à actividade maliciosa.

- O programa protege o computador de rootkits e programas de ligações telefónicas, bloqueia faixas de anúncios, janelas popup e scripts maliciosos transferidos de páginas da Internet e também detecta sites de phishing.
- A tecnologia do Anti-vírus de Ficheiros foi melhorada para diminuir a carga sobre o CPU e aumentar a velocidade de verificação de ficheiros, utilizando as tecnologias iChecker™ e iSwift™. Ao funcionar desta forma, o programa elimina as verificações repetidas dos mesmos ficheiros.
- O processo de verificação decorre agora, em segundo plano, enquanto usa o computador. Uma verificação pode levar algum tempo e usar recursos do sistema, mas o utilizador pode agora continuar a usar o computador. Se qualquer operação necessitar de recursos do sistema, a verificação de vírus pára até que essa operação seja concluída. A verificação continua depois no ponto onde a deixou.
- As áreas críticas do computador, que podem levar a consequências sérias se estiverem infectadas, têm o seu próprio processo em separado. Pode configurar este processo para ser executado sempre que o sistema se inicia.
- A protecção dos sistemas e-mail em relação a programas maliciosos e spam foi significativamente melhorada. O programa verifica estes protocolos quanto à existência e-mails com vírus e spam:
    - IMAP, SMTP, POP3, independentemente do cliente de e-mail que usar
    - NNTP (apenas verificação de vírus), independentemente do cliente de e-mail
    - MAPI, HTTP (utilizando extensões para o MS Outlook e o The Bat!!
- Estão disponíveis extensões especiais para os clientes de e-mail mais comuns, como o Microsoft Office Outlook, o Microsoft Outlook Express (programa de e-mail do Windows) e o The Bat!. Pode configurar,

directamente a partir do cliente de e-mail, a protecção, tanto contra vírus, como contra spam.

- Agora o Anti-Spam tem um modo de treino, com base no algoritmo de Bayes, que aprende ao monitorizar a forma como lida com os e-mails. Também fornece a máxima flexibilidade à configuração da detecção de spam – por exemplo pode criar listas pretas e brancas de endereços e frases-chave que classificam o e-mail como spam.

O Anti-Spam usa uma base de dados de phishing. Pode filtrar e-mails concebidos para obter informação confidencial de natureza financeira.

- O programa filtra o tráfego de entrada e saída, segue e bloqueia ameaças de ataques de rede comuns e deixa-o usar a Internet em modo Furtivo.
- Quando utilizar uma combinação de redes, poderá também definir em que redes confia totalmente e quais as que quer monitorizar com cuidado extremo.
- A função de notificação do utilizador (ver 17.11.1 na pág. 278) foi alargada para determinados eventos de protecção. Pode seleccionar o método de notificação, escolhendo entre e-mails, notificações sonoras, mensagens que se abrem e registando o evento.
- Foi adicionada a verificação para os dados transmitidos através de ligações seguras SSL.
- O programa juntou funções de autodefesa, incluindo a protecção contra acesso remoto não-autorizado por parte de serviços Anti-vírus e protecção das definições do programa através de password. Estas funções ajudam a evitar que programas maliciosos, hackers e utilizadores não-autorizados desactivem a protecção.
- Também pode criar um disco de recuperação, a partir do qual pode reiniciar o seu sistema operativo após um surto de vírus e analisar o seu computador quanto à presença de código malicioso.
- Agora o sistema de protecção tem a opção da administração remota centralizada, utilizando uma interface de administração adicional através do Kaspersky Administration Kit.

Novas funções de interface do programa

- A nova interface do Kaspersky Anti-virus para Windows Workstations torna as funções do programa mais simples e fáceis de usar. Também pode mudar a aparência do programa, utilizando o seu próprio grafismo e esquemas de cor.
- Ao utilizar o programa, este fornece, regularmente, dicas: o Kaspersky Anti-virus para Windows Workstations exibe mensagens informativas

sobre o nível de protecção, acompanha o seu funcionamento com dicas e inclui uma secção minuciosa de ajuda.

Novas funções de actualização do programa

- Esta versão do programa estreia o nosso melhorado procedimento de actualização: agora o Kaspersky Anti-virus verifica, automaticamente, se existem actualizações na origem de actualização. Se encontrar novas actualizações, o Anti-vírus transfere-as e instala-as no computador.
- O programa apenas transfere as actualizações que ainda não tiver. Isto reduz, em cerca de 10 vezes, o tráfego de transferência de actualizações.
- As actualizações são transferidas a partir da origem de actualização mais eficiente.
- Agora poderá escolher não usar um servidor de proxy, se as actualizações do programa forem transferidas a partir de uma fonte local. Isto reduz, consideravelmente, o tráfego no servidor de proxy.
- O programa tem uma função de reversão das actualizações que pode restaurar até à versão anterior das assinaturas se as assinaturas de ameaças estiverem danificadas ou houver um erro ao copiá-las.
- Foi adicionada ao Actualizador uma ferramenta que copia as actualizações para uma pasta local para as tornar acessíveis a outros computadores da rede. Isto reduz o tráfego de Internet.

2.2. Como é constituída a Protecção do Kaspersky para Windows Workstations

O Kaspersky Anti-virus para Windows Workstations é concebido tendo em conta as fontes de ameaças. Por outras palavras, cada componente do programa trata de uma dada ameaça, controlando-a e executando os passos necessários para prevenir os efeitos maliciosos daquela fonte nos dados do utilizador. Esta configuração torna a Solução de Segurança flexível, com opções de configuração fáceis para todas as componentes, que obedeçam às necessidades de um utilizador específico ou de uma empresa como um todo.

O Kaspersky Anti-virus para Windows Workstations inclui:

- Componentes de protecção (ver 2.2.1 na pág. 26) que permitem uma defesa global em todos os canais de transmissão e intercâmbio de dados no seu computador, em tempo real.
- Tarefas de verificação de vírus (ver 2.2.2 na pág. 28) que verificam a existência de vírus no computador ou em ficheiros individuais, pastas, discos ou regiões.
- Ferramentas de suporte (ver 2.2.3 na pág. 29) que dão suporte ao programa e aumentam a sua funcionalidade.

2.2.1. Componentes de protecção

Estas componentes de protecção defendem o seu computador em tempo real:

Anti-vírus de Ficheiros

Um sistema de ficheiros pode conter vírus e outros programas perigosos. Os programas maliciosos podem ser guardados no sistema de ficheiros durante anos, depois de se terem instalado através de uma disquete ou pela Internet, sem se mostrarem. Mas bastará abrir o ficheiro infectado e o vírus é imediatamente activado.

O *Anti-vírus de Ficheiros* é a componente que controla o sistema de ficheiros do computador. Analisa todos os ficheiros que possam ser abertos, executados ou guardados no computador e em unidades de disco ligadas. De cada vez que se aceder a um ficheiro, Kaspersky Anti-Virus intercepta-o e verifica o ficheiro quanto à existência de vírus conhecidos. Se, por qualquer razão, um ficheiro não puder ser desinfectado, este será apagado, sendo criada uma cópia do mesmo que é guardada na Cópia de Segurança (ver 17.2 na pág. 243) ou sendo movido para a Quarentena (ver 17.1 na pág. 239).

Anti-vírus de E-Mail

O correio electrónico é amplamente usado por hackers para espalhar programas nocivos. É um dos métodos mais comuns para espalhar worms. Por isso, é extremamente importante controlar todos os e-mails.

O *Anti-vírus de E-Mail* é a componente que verifica todo o correio de entrada e de saída no computador. Procura programas nocivos nos e-mails. O programa apenas garante ao destinatário o acesso ao e-mail se este estiver livre de objectos perigosos.

Anti-vírus de Internet

Quando abre páginas na Internet arrisca-se a infectar o seu computador com vírus instalados nessas páginas com os scripts armazenados nas

páginas da Internet. Também se arrisca a transferir um ficheiro perigoso para o seu computador.

O *Anti-vírus de Internet* é especialmente concebido para antecipar essas situações. Esta componente intercepta e bloqueia scripts em locais da Internet se estes constituírem uma ameaça. Todo o tráfego HTTP é minuciosamente controlado.

Defesa Pró-activa

A cada dia, existem mais e mais programas nocivos. Estão a tornar-se mais complexos, combinando alguns tipos e os métodos que usam para se espalharem alteram-se, tornando-os cada vez mais difíceis de detectar.

Para detectar um novo programa malicioso antes deste ter tempo de causar qualquer dano, a Kaspersky Lab desenvolveu uma componente especial, a *Defesa Pró-activa*. É concebida para monitorizar e analisar do comportamento de todos os programas instalados no computador. O Kaspersky Anti-virus toma uma decisão baseada nas acções executadas pelo programa: é potencialmente perigoso? A Defesa Pró-activa protege o computador tanto de vírus conhecidos, como de novos vírus que tenham ainda que ser descobertos.

Anti-Spy

Recentemente, têm se tornado ainda mais comuns os programas que exibam publicidade sem o utilizador a ter pedido (faixas de anúncios e janelas de popup), programas que marcam números de serviços pagos da Internet sem a autorização do utilizador, a administração remota e ferramentas de monitorização, programas de brincadeiras, etc.

O *Anti-Spy* investiga estas acções no computador e bloqueia-as. Por exemplo, a componente bloqueia faixas de anúncios e janelas que se abrem (janelas de popup), um incómodo quando se está na Internet, bloqueia programas que tentem marcar um número de telefone e analisa conteúdos de phishing nas páginas da Internet.

Anti-Hacker

Os Hackers usarão qualquer furo potencial para invadir o computador, quer seja numa rede aberta ou ao transmitir dados de computador para computador, etc.

O *Anti-Hacker* é a componente concebida para proteger o computador enquanto usa a Internet e outras redes. Controla as ligações de entrada e de saída e verifica portas e pacotes de dados.

Anti-Spam

Apesar de não ser uma ameaça directa ao computador, o spam aumenta a carga em servidores de e-mail, enche a caixa de correio e gasta-lhe tempo, provocando assim prejuízos financeiros.

A componente *Anti-Spam* liga-se ao cliente e-mail instalado no computador e procura assuntos de spam em todo o correio de entrada. Todos os e-mails que contêm spam são marcados com um cabeçalho especial. O Anti-Spam também pode ser configurado para processar spam da forma que pretender (apagar, mover para uma pasta especial, etc.).

2.2.2. Tarefas de verificação de vírus

É extremamente importante verificar, periodicamente, a existência de vírus no computador, juntamente com o controlo constante de todas as vias potenciais para programas nocivos. Isto é necessário para eliminar a possibilidade de disseminação de programas maliciosos que ainda não foram descobertos pelas componentes de segurança, porque o nível de segurança é baixo ou por outras razões.

O Kaspersky Anti-virus para Windows Workstations configura, por defeito, as seguintes tarefas para procurar vírus:

Áreas críticas

Procura vírus em todas as áreas críticas do computador. Estas incluem: a memória do sistema, programas carregados ao iniciar, sectores de arranque do disco rígido e os directórios do sistema *Microsoft Windows*. A tarefa tenta detectar, rapidamente, os vírus activos no sistema, sem fazer uma verificação completa do computador.

O Meu Computador

Procura vírus no seu computador com uma inspecção minuciosa de todas as unidades de disco, memória e ficheiros.

Objectos de inicialização

Procura vírus em todos os programas que sejam, automaticamente, carregados ao iniciar, e ainda na memória RAM e nos sectores de arranque dos discos rígidos.

Também tem a opção de criar outras tarefas de procura de vírus e agendá-las. Por exemplo, pode criar uma tarefa de verificação de bases de dados de e-mail uma vez por semana ou uma tarefa de verificação de vírus para a pasta **Os Meus Documentos**.

2.2.3. Ferramentas do programa

O Kaspersky Anti-virus para Windows Workstations inclui uma quantidade de ferramentas de suporte. São concebidas para fornecer suporte ao software em tempo real, expandindo as capacidades do programa e assistindo-o enquanto trabalha.

Actualizador

Para estar sempre preparado para qualquer ataque de hacker e pronto para apagar um vírus ou outro programa perigoso, o Kaspersky Anti-virus para Windows Workstations precisa de se manter actualizado. A componente do *Actualizador* está concebida precisamente para fazer isso. É responsável por actualizar as assinaturas de ameaças do Kaspersky Anti-virus para Windows Workstations e os módulos do programa.

A função de Distribuição de Actualizações consegue guardar numa pasta local as actualizações das assinaturas de ameaças e dos módulos da aplicação recolhidas a partir dos servidores de actualização da Kaspersky Lab. Em seguida torna-as acessíveis a outros computadores da rede para poupar na largura de banda.

Ficheiros de dados

Durante a sua execução, cada componente de protecção, tarefa de verificação de vírus e actualização do programa cria um relatório próprio. Os relatórios contêm informação sobre operações concluídas e os seus resultados. Ao usar a função *Relatórios*, estará sempre actualizado sobre o funcionamento de todas as componentes do Kaspersky Anti-virus para Windows Workstations. Se surgirem problemas, poderá enviar os relatórios à Kaspersky Lab para os nossos especialistas poderem estudar a situação em maior detalhe e ajudá-lo com a maior rapidez possível.

O Kaspersky Anti-virus para Windows Workstations envia todos os ficheiros suspeitos de serem perigosos para uma área especial de *Quarentena*. Aqui são guardados encriptados para evitar a infecção do computador. Pode fazer uma verificação de vírus nestes objectos, restaurá-los para os seus locais anteriores, apagá-los ou adicionar, por si próprio, os ficheiros à Quarentena. Após terminar a verificação, todos os ficheiros, que se considere não estarem infectados, são automaticamente restaurados para os seus locais anteriores.

A *Cópia de Segurança* guarda cópias de ficheiros desinfectados e apagados pelo programa. Estas cópias são criadas caso queira restaurar os ficheiros ou informação sobre a infecção. As cópias de segurança dos ficheiros são também guardadas de forma encriptada para evitar mais infecções.

Pode restaurar manualmente um ficheiro da Cópia de Segurança para o local original e apagar a respectiva cópia.

Disco de recuperação

O Kaspersky Anti-virus para Windows Workstations inclui uma função especial onde pode criar um disco de recuperação. A criação desse disco fornece um plano de segurança caso os ficheiros de sistema sejam danificados por um ataque de vírus e se for impossível iniciar o sistema operativo. Neste caso, ao usar o disco de recuperação, poderá iniciar o computador e restaurar o sistema para o estado anterior à acção maliciosa.

Suporte

Todos os utilizadores registados do Kaspersky Anti-virus podem beneficiar do nosso serviço de suporte técnico. Para saber exactamente onde pode obter suporte técnico, use a função *Suporte*.

Utilizando estas ligações, pode aceder ao fórum de utilizadores da Kaspersky Lab e a uma lista de perguntas frequentes que poderão ajudá-lo a resolver o seu problema. Para além disso, ao completar o formulário no site, pode enviar para o Suporte Técnico uma mensagem sobre o erro ou falha no funcionamento da aplicação.

Também poderá aceder ao suporte técnico on-line, e, claro, os nossos funcionários estarão sempre prontos a dar-lhe assistência, por telefone, sobre o Kaspersky Anti-virus.

2.3. Requisitos de hardware e software de sistema

Para o Kaspersky Anti-virus para Windows Workstations 6.0 funcionar convenientemente, o computador deve obedecer a estes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço livre em disco
- CD-ROM (para instalação do Kaspersky Anti-virus para Windows Workstations 6.0 pelo CD de instalação)
- Microsoft Internet Explorer 5.5 ou superior (para actualização de assinaturas de ameaças e módulos do programa através da Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Processador Intel Pentium 300 MHz ou superior (ou compatível)
- 64 MB de RAM

Microsoft Windows 2000 Professional (Service Pack 4 ou superior), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 ou superior), Microsoft Windows XP Professional Edição x64:

- Processador Intel Pentium 300 MHz ou compatível
- 128 MB de RAM

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Intel Pentium 800 MHz 32-bit (x86)/ 64-bit (x64) superior (ou compatível).
- 512 MB de RAM

2.4. Pacotes de software

Pode adquirir o Kaspersky Anti-virus para Windows Workstations nos nossos representantes numa caixa ou através da loja da Internet (por exemplo, www.kaspersky.com, na secção **Loja on-line**).

Se comprar a versão do programa em caixa, esta inclui:

- Um envelope selado com um CD de instalação, contendo os ficheiros de programa
- Uma chave de licença, incluída no pacote de instalação ou numa disquete especial, ou um código de activação colado ao CD de instalação
- Um manual de utilizador
- O Contrato de Licença do Utilizador Final (CLUF)

Antes de romper o selo do envelope de instalação do disco, leia cuidadosamente o CLUF.

Se comprar o Kaspersky Anti-virus para Windows Workstations numa loja online, estará a copiar o produto a partir da página da Kaspersky Lab (**Downloads → Product Downloads**). Poderá transferir o manual de utilizador na secção **Downloads → Documentation**.

Ser-lhe-á enviado uma chave de licença ou um código de activação por e-mail, depois de ter efectuado o pagamento.

O Contrato de Licença do Utilizador Final é um acordo legal entre você e a Kaspersky Lab, que especifica os termos pelos quais poderá usar o software que adquiriu.

Leia o CLUF cuidadosamente.

Se não concordar com os termos do CLUF, poderá devolver o produto embalado ao revendedor onde o comprou e ser reembolsado pela quantidade que pagou pelo programa. Se o fizer, o envelope selado do disco de instalação deve permanecer selado.

Ao abrir o disco selado de instalação, aceitará todos os termos do CLUF.

2.5. Suporte para utilizadores registados

A Kaspersky Lab fornece aos seus utilizadores registados uma série de serviços que tornam o Kaspersky Anti-virus para Windows Workstations mais eficaz.

Após a activação do programa, torna-se num utilizador registado do programa e terá os seguintes serviços disponíveis até a licença expirar:

- Novas versões grátis do programa
- Consultas sobre questões de instalação, configuração e funcionamento do programa, por telefone e e-mail
- Notificações sobre edições do produto da Kaspersky Lab e novos vírus (estes serviços são para utilizadores que subscrevam os mailings de novidades da Kaspersky Lab)

A Kaspersky Lab não dá Suporte Técnico sobre uso e funcionamento do sistema operativo ou outros produtos para além do seu.

CAPÍTULO 3. INSTALAÇÃO DO KASPERSKY ANTI-VIRUS PARA WINDOWS WORKSTATIONS 6.0

Existem várias formas para instalar o Kaspersky Anti-Virus 6.0 para Windows Workstations:

- Instalação Local: instale a aplicação num único anfitrião. Para executar e concluir a instalação, é necessário ter acesso directo ao anfitrião em questão. Pode efectuar uma instalação local através de um dos seguintes modos:
    - uma instalação interactiva, utilizando o Assistente de Instalação da aplicação (ver 3.1 na pág. 34); este modo requer a inserção de dados pelo utilizador para prosseguir com a instalação;
    - uma instalação não interactiva executada a partir da linha de comandos, utilizando as predefinições e não necessitando de qualquer inserção de dados por parte do utilizador para prosseguir com a instalação (ver 3.3, pág. 48).
- Instalação Remota: instala a aplicação em computadores em rede, de forma remota a partir de uma estação de trabalho do administrador com a utilização do:
    - Solução de software Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration Kit);
    - Políticas de domínios de grupo Microsoft Windows Server 2000/2003 (ver 3.4, pág. 49).

Recomenda-se que encerre todas as aplicações em execução antes da instalação do Kaspersky Anti-Virus (inclusive numa instalação remota).

Caso já tenha instalado o Kaspersky Anti-Virus 5.0, este será removido e actualizado para o Kaspersky Anti-Virus 6.0 quando executar o procedimento de instalação (ver 3.5, pág. 51 para mais detalhes). As actualizações para compilações mais recentes (versões inferiores) no Kaspersky Anti-Virus 6.0 são transparentes.

3.1. Procedimento de instalação usando o Assistente de Instalação

Para instalar o Kaspersky Anti-virus para Windows Workstations no seu computador, abra o ficheiro do Windows Installer no CD de instalação.

> Nota:
>
> Instalar a aplicação com um pacote de instalação transferido da Internet não é diferente da instalação a partir do CD de instalação.

Aparecerá um assistente para a instalação do programa. Cada janela contém um conjunto de botões para navegar ao longo do processo de instalação. Aqui está uma breve explicação das suas funções:

- **Seguinte** – aceita uma acção e avança para a próxima fase da instalação.
- **Anterior** – volta à fase anterior da instalação.
- **Cancelar** – cancela a instalação do produto.
- **Concluir** – completa o procedimento de instalação do programa.

Analisemos, mais detalhadamente, as fases do procedimento de instalação do programa.

Passo 1. Procurar as condições do sistema necessárias para instalar o Kaspersky Anti-virus para Windows Workstations

Antes do programa ser instalado no seu computador, o ficheiro de instalação procura no seu computador o sistema operativo e os pacotes necessários para instalar o Kaspersky Anti-virus para Windows Workstations. Também procura outros programas necessários e verifica se os seus direitos de utilizador lhe permitem instalar o software.

Se alguns destes requisitos falhar, o programa exibirá uma mensagem informando-o desse facto. Antes de instalar o Kaspersky Anti-virus para Windows Workstations, recomenda-se a instalação dos pacotes de serviço necessários através do **Windows Update** e dos programas necessários.

Passo 2. Janela de Boas-vindas da Instalação

Se o seu sistema cumprir todos os requisitos, quando abrir o ficheiro de instalação, aparecerá de imediato uma janela de instalação com informação sobre o início da instalação do Kaspersky Anti-virus para Windows Workstations.

Para prosseguir a instalação, clique no botão **Seguinte**. Pode cancelar a instalação clicando no botão **Cancelar**.

Passo 3. Visualizar o Contrato de Licença do Utilizador Final

A próxima janela contém um Contrato de Licença do Utilizador Final que é acordado entre você e a Kaspersky Lab. Leia tudo com muita atenção, e se concordar com todas as condições do acordo, seleccione **Eu aceito os termos do Contrato de Licença** e clique no botão **Seguinte**. A instalação prosseguirá.

Para cancelar a instalação clique em **Cancelar**.

Passo 4. Seleccionar uma pasta de instalação

O próximo passo da instalação do Kaspersky Anti-virus para Windows Workstations determina onde o programa será instalado no seu computador. O caminho predefinido é o seguinte:

- **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 para Windows Workstations** – para sistemas 32-bit
- **<Drive>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 para Windows Workstations** – para sistemas 64-bit

Poderá especificar uma pasta diferente, clicando no botão **Procurar** e seleccionando-a na janela de selecção da pasta ou inserindo o atalho para a pasta no campo disponível.

Lembre-se que se introduzir, manualmente, o caminho completo para a pasta de instalação, este não deverá exceder os 200 caracteres ou conter caracteres especiais.

Para prosseguir a instalação, clique no botão **Seguinte**.

Passo 5. Utilizar Definições Guardadas na Instalação

Neste passo, é-lhe perguntado para especificar se deseja utilizar as definições de segurança ou assinaturas de ameaças anteriormente guardadas, caso

tenham sido guardadas quando removeu do seu computador uma instalação anterior do Kaspersky Anti-Virus 6.0.

Vamos analisar com maior detalhe sobre como utilizar as opções acima descritas.

Se já teve instalada no seu computador uma outra versão ou compilação do Kaspersky Anti-Virus para Windows Workstations e guardou as suas assinaturas de ameaças quando a desinstalou, pode utilizar essas assinaturas na versão actual. Para o fazer, assinale a opção ☑ **Assinaturas de ameaças**. As assinaturas de ameaças incluídas com a instalação do programa não serão copiadas para o servidor.

Para utilizar as definições de protecção que configurou e guardou de uma versão anterior, assinale a opção ☑ **Definições de protecção**.

Passo 6. Seleccionar o tipo de instalação

Nesta fase, seleccione a quantidade de recursos do programa que deseja instalar no seu computador. Tem três opções:

Completa. Se seleccionar esta opção, todas as componentes do Kaspersky Anti-virus para Windows Workstations serão instaladas. A instalação irá recomeçar com o Passo 8.

Personalizar. Se seleccionar esta opção, terá de seleccionar as componentes do programa que deseja instalar. Para mais informação, veja o Passo 7.

Recursos do Anti-vírus. Esta opção instala as componentes que o protegem contra vírus. O Anti-Hacker, Anti-Spam e o Anti-Spy não serão instalados.

Para seleccionar um tipo de instalação, clique no botão apropriado.

Passo 7. Seleccionar as componentes do programa a instalar

> Este passo apenas ocorrerá se seleccionar o tipo de instalação **Personalizar**.

Se seleccionou a instalação **Personalizar**, terá de seleccionar as componentes do Kaspersky Anti-virus para Windows Workstations que deseja instalar. Por defeito, estão seleccionados para instalação o Anti-vírus de Ficheiros, a componente de verificação de vírus e conector ao Agente de Administração para administração remota através do Kaspersky Administration Kit .

Para seleccionar as componentes que deseja instalar, clique com o botão esquerdo do rato no ícone perto do nome da componente e, no menu de contexto, seleccione **Será instalado no disco rígido local** a partir do menu

aberto. Na parte inferior da janela de instalação do programa, encontrará mais informação sobre o tipo de protecção que a componente fornece e sobre o espaço de disco necessário para a instalação.

Se não deseja instalar uma componente, no menu de contexto seleccione **O recurso estará indisponível**. Lembre-se que, ao escolher não instalar uma componente, se priva da protecção contra um vasto leque de programas perigosos.

Após seleccionar as componentes que deseja instalar, clique em **Seguinte**. Para regressar à lista dos programas predefinidos a serem instalados, clique **Repor**.

Passo 8. Desactivar a firewall do Microsoft Windows

Só passará por esta fase se estiver a instalar o Kaspersky Anti-Virus para Windows Workstations num computador com a firewall integrada activada e estiver a instalar o Anti-Hacker

Neste passo, o Kaspersky Anti-Virus para Windows Workstations pergunta-lhe se quer desactivar a Firewall do Windows, já que o Anti-Hacker, que está incluído no Kaspersky Anti-Virus para Windows Workstations, lhe dá a protecção total por firewall e não há necessidade de uma protecção adicional do sistema operativo.

Se desejar utilizar o Anti-Hacker como a sua protecção de firewall, clique em **Seguinte**. A Firewall do Windows será, automaticamente, desactivada.

Se desejar utilizar a Firewall do Windows, seleccione ☑ **Manter a Firewall do Windows activada**. Se seleccionar esta opção, o Anti-Hacker será instalado, mas desactivado para evitar conflitos de programas.

Passo 9. Procurar outros programas de anti-vírus

Nesta fase, o ficheiro de instalação procura outros produtos anti-vírus instalados no seu computador, incluindo produtos da Kaspersky Lab, que podem causar problemas de compatibilidade com o Kaspersky Anti-virus para Windows Workstations.

Se o ficheiro de instalação detectar algum desses programas, mostrará no ecrã uma lista com os mesmos. O programa perguntará se deseja desinstalá-los antes de prosseguir com a instalação.

Na lista de aplicações anti-vírus detectadas, pode seleccionar a desinstalação manual ou automática (apenas os produtos da Kaspersky Lab serão automaticamente apagados).

Para prosseguir com a instalação, clique no botão **Seguinte**.

Passo 10. Concluir a instalação do seu programa

Nesta fase, o programa vai lhe pedir que conclua a instalação do programa no seu computador.

Não é aconselhável desmarcar a caixa ☑ **Activar Auto-Defesa antes da instalação** ao instalar, inicialmente, o Kaspersky Anti-virus 6.0. Ao activar os módulos de protecção, poderá reverter, correctamente, a instalação se ocorrerem erros ao instalar o programa. Se estiver a reinstalar o programa, recomendamos que desmarque esta opção.

> Se a aplicação for instalada de forma remota, através do **Windows Remote Desktop**, recomendamos que assinale a caixa ☑ **Activar Auto-Defesa antes da instalação**. Caso contrário, o procedimento de instalação pode não ser concluído ou correctamente concluído.

Para prosseguir com a instalação, clique no botão **Seguinte**.

> Aviso!
>
> Quando estão a ser instaladas as componentes do Kaspersky Anti-Virus que interceptam o tráfego de rede, as actuais ligações de rede são interrompidas. A maioria delas será recuperada após algum tempo.

Passo 11. Concluir o procedimento de instalação

A janela **Concluir Instalação** contém informação sobre como concluir o processo de instalação do Kaspersky Anti-virus.

Para iniciar o assistente de configuração, clique no botão **Seguinte** (ver 3.2, pág. 38).

Se a instalação for terminada com sucesso, precisará de reiniciar o seu computador e uma mensagem no ecrã dir-lhe-á isso mesmo.

3.2. Assistente de Configuração

O Assistente de Configuração do Kaspersky Anti-Virus para Windows Workstations 6.0 inicia-se no final da instalação do programa. Está concebido para o ajudar a configurar as definições iniciais do programa que estão em conformidade com as características e usos do seu computador.

A interface do Assistente de Configuração está concebida como um Assistente padrão do Windows e consiste numa série de passos que poderá executar utilizando os botões **Anterior** e **Seguinte** ou concluir utilizando o **botão Concluir**. O botão **Cancelar** parará o Assistente em qualquer momento.

Poderá ignorar esta fase inicial de definições, ao instalar o programa, fechando a janela do Assistente. Futuramente, poderá voltar a ela a partir da interface do programa se restaurar as definições predefinidas para o Kaspersky Anti-virus para Windows Workstations (ver 17.3 na pág. 245).

3.2.1. Utilizar ficheiros guardados da Versão 5.0

Esta janela do assistente aparece quando instala a aplicação em substituição da versão 5.0 do Kaspersky Anti-virus. Ser-lhe-á pedido para seleccionar quais os dados utilizados pela versão 5.0 que deseja importar para a versão 6.0. Isso pode incluir ficheiros da quarentena ou da cópia de segurança ou ainda definições de protecção.

Para utilizar estes dados na Versão 6.0, seleccione as caixas necessárias.

3.2.2. Activar o programa

Antes de tentar activar o programa, certifique-se de que as definições de data do sistema do computador correspondem à hora e data actuais.

O programa é activado instalando uma chave de licença que o Kaspersky Anti-Virus irá usar para procurar uma licença e determinar a data de validade da mesma.

A chave de licença contém informações sobre o sistema necessárias para o funcionamento de todas as funções do programa e outra informação:

- Informação de Suporte (quem fornece o apoio e onde obtê-lo)
- Nome, número, e data de validade da sua licença

3.2.2.1. Seleccionar o método de activação do programa

Dependendo se possui uma chave para o Kaspersky Anti-virus ou se precisa de obter uma a partir do servidor da Kaspersky Lab, existem várias opções para activar o programa:

Activar através do código de activação. Seleccionar esta opção de activação se tiver comprado a versão completa do programa e lhe tiver sido dado um código de activação. Utilizando este código de activação, você

obterá um ficheiro de chave que dará acesso a todas as funcionalidades da aplicação durante o prazo efectivo do acordo de licença.

- **Activar versão de avaliação.** Seleccione esta opção de activação se deseja instalar a versão de avaliação do programa antes de decidir comprar a versão comercial. Ser-lhe-á fornecida uma chave gratuita válida durante um período especificado no acordo de licença da versão de avaliação.
- **Aplicar a chave de licença existente.** Active a aplicação, usando um ficheiro da chave de licença do Kaspersky Anti-virus 6.0.
- **Activar mais tarde.** Se escolher esta opção, saltará a fase de activação. O Kaspersky Anti-virus para Windows Workstations 6.0 será instalado no seu computador e terá acesso a todas as funcionalidades do programa, excepto as actualizações (só poderá actualizar as assinaturas de ameaças quando instalar o programa).

As primeiras duas opções de activação utilizam um servidor de Internet da Kaspersky Lab, o que requer uma ligação à Internet. Antes de activar, certifique-se de que altera as suas definições de rede, se necessário, (ver 16.4.3 na pág. 233) na janela que se abre quando clica em **Definições de LAN**. Para mais informação detalhada sobre as definições de configuração da rede, contacte o seu administrador de sistema ou o provedor de serviços de Internet.

Se não tiver ligação à Internet quando instalar o programa, pode activar a aplicação mais tarde (ver 17.5 na pág. 264) utilizando a interface da mesma ou pode utilizar o acesso à Internet de outro computador para se registar no site de Suporte Técnico da Kaspersky Lab e obter a chave com o código de activação.

3.2.2.2. Inserir o código de activação

Para activar o programa, você tem que inserir um código de activação. Se tiver comprado o programa através da Internet, receberá o código de activação por e-mail. Se comprou o software numa versão de embalagem, encontrará o código de activação no envelope do CD de instalação.

O código de activação é uma sequência de números e letras separados por traços em quatro secções, cada uma das quais com cinco caracteres, sem espaços. Por exemplo, 11AA1-11AAA-1AA11-1A111. Note que o código tem ser inserido em caracteres latinos.

Introduza a sua informação de contacto na parte inferior da janela: nome completo, endereço de correio electrónico, país e cidade onde reside. Esta informação poderá ser pedida para identificar um utilizador registado, se por exemplo a chave seja perdida ou roubada. Se isso acontecer, a sua informação de contacto permitir-lhe-á obter uma nova chave de licença.

3.2.2.3. Obter um Ficheiro da Chave

O Assistente de Configuração comunica com os servidores da Kaspersky Lab e envia-lhes os seus dados de registo (o código de activação e os dados pessoais), que são verificados no servidor.

Se o código de activação passar a verificação, o Assistente recebe um ficheiro da chave. Se instalar a versão de avaliação do programa, o Assistente de Configuração receberá um ficheiro da chave de avaliação sem código de activação.

O ficheiro obtido será automaticamente instalado para utilizar o programa e verá uma janela "Activação concluída" com informação detalhada sobre a chave actualmente utilizada.

Se o código de activação não passar a inspecção, verá uma mensagem no ecrã. Se tal acontecer, para mais informações, contacte o vendedor do software ao qual comprou o programa, para obter informação.

3.2.2.4. Seleccionar o ficheiro da chave de licença

Se possui um ficheiro da chave de licença para o Kaspersky Anti-virus para Windows Workstations 6.0 , o Assistente perguntar-lhe-á se o deseja instalar. Se quiser, utilize o botão **Procurar** e, na janela de selecção do ficheiro, seleccione o caminho para o ficheiro da chave com a extensão *.key*.

Depois de ter instalado a chave com sucesso, visualizará a informação sobre a licença na parte inferior da janela: nome da pessoa na qual o software está registado, número da licença, tipo de licença (completa, teste beta, demo, etc.), e a data de validade para a chave.

3.2.2.5. Concluir a activação do programa

O Assistente de Configuração informá-lo-á de que o programa foi activado com sucesso. Também disponibilizará informação sobre a chave da licença instalada: nome da pessoa na qual o software está registado, número da licença, tipo de licença (completa, teste beta, demo, etc.), e a data de validade para a chave.

3.2.3. Seleccionar um modo de protecção

Nesta janela, o Assistente de Configuração pede-lhe que seleccione o modo de protecção segundo o qual o programa será executado:

Básica. Esta é a opção predefinida e foi desenhada para utilizadores que não têm experiência muito aprofundada com computadores ou programas de anti-vírus. Esta opção atribui a todas as componentes do programa os seus níveis de segurança recomendados e apenas informa o utilizador acerca de eventos perigosos, tais como a detecção de código malicioso ou a execução de acções perigosas.

Interactiva. Comparativamente ao Modo Básico, este modo fornece uma protecção mais personalizada dos dados do seu computador. Pode registar tentativas para alterar definições do sistema, actividades suspeitas no sistema e actividade não autorizada na rede.

Todas as actividades acima listadas podem ser sinais de programas maliciosos ou actividades padrão para alguns dos programas que você usa no seu computador. Você terá que decidir, para cada caso em separado, se essas actividades devem ser permitidas ou bloqueadas.

Se escolher este modo, especifique em que contextos deve ser usado:

- [x] **Activar Modo de Treino do Anti-Hacker** – pede ao utilizador que tome decisões quando os programas instalados no seu computador tentam ligar-se a um determinado recurso de rede. Você pode permitir ou bloquear essa ligação e configurar uma regra do Anti-Hacker para esse programa. Se desactivar o Modo de Treino, o Anti-Hacker é executado com as definições de protecção mínima, o que significa que permite que todas as aplicações tenham acesso a recursos de rede.

- [x] **Activar a Monitorização do Registo** – pede ao utilizador que tome uma decisão se foram detectadas tentativas para alterar as chaves de registo do sistema.

> Se a aplicação estiver instalada num computador com Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou Microsoft Windows Vista x64, as definições do modo interactivo abaixo listadas não estarão disponíveis.

- [x] **Activar Defesa Pró-activa Alargada** – permite a análise de toda a actividade suspeita de aplicações no sistema, incluindo a abertura de navegadores de Internet com definições de linhas de comando, a intrusão em processos de aplicações e ganchos em janelas (por defeito, estas definições estão desactivadas.

3.2.4. Configurar as definições de actualização

A segurança do seu computador depende directamente da actualização regular das assinaturas de ameaças e dos módulos do programa. Nesta janela, o Assistente de Configuração pede-lhe que seleccione um tipo de actualização do programa e que configure um agendamento para as actualizações.

- **Automaticamente**. O Kaspersky Anti-virus verifica, em intervalos especificados, se existem actualizações na origem de actualização. As verificações podem ser definidas para serem mais frequentes durante surtos de vírus e menos frequentes quando esses surtos terminam. Quando o Anti-vírus detecta novas actualizações, transfere-as e instala-as no computador. Esta é a opção predefinida.
- **A cada 2 hora(s)**. As actualizações acontecerão automaticamente segundo o agendamento de actualizações definido. Poderá configurar o agendamento das actualizações, clicando em **Alterar**.
- **Manualmente**. Se escolher esta opção, você mesmo fará as actualizações do programa.

Tenha em atenção que as assinaturas de ameaças e os módulos do programa incluídos no software poderão estar desactualizados na altura em que instalar o programa. É por isso que recomendamos a transferência das últimas actualizações do programa. Para fazer isso, clique em **Actualizar Agora**. Deste modo, o Kaspersky Anti-virus para Windows Workstations irá transferir as actualizações necessárias a partir dos servidores de actualização e instalá-las-á no seu computador.

Se desejar configurar as actualizações (definir propriedades da rede, seleccionar o recurso a partir do qual as actualizações serão transferidas, configurar a execução de tarefas com uma determinada conta de utilizador ou activar a opção de distribuição de actualizações), clique em **Definições**.

3.2.5. Configurar verificações de vírus agendadas

Uma das tarefas-chave para proteger o seu computador é a verificação de áreas seleccionadas do seu computador, procurando ficheiros maliciosos.

Quando você instala o Kaspersky Anti-virus para Windows Workstations, são criadas três tarefas para verificação de vírus. Nesta janela, o Assistente de Configuração pede-lhe para escolher uma definição de tarefa de verificação.

Objectos de Inicialização

Por defeito, quando o Kaspersky Anti-virus é iniciado, este verifica, automaticamente, objectos de inicialização. Poderá editar as definições de agendamento noutra janela, clicando em **Alterar**.

Áreas Críticas

Por forma a analisar, automaticamente, as áreas críticas do seu computador (memória do sistema, ficheiros de inicialização, sectores de arranque, pastas de sistema do Windows), assinale a caixa apropriada. Poderá configurar o agendamento das actualizações clicando em **Alterar**.

A definição predefinida, para esta verificação automática, está desactivada.

O Meu Computador

Por forma a executar, automaticamente, uma verificação total do seu computador, assinale a caixa apropriada. Poderá configurar o agendamento das actualizações clicando em **Alterar**.

A definição predefinida para executar esta tarefa, de acordo com o agendamento, está desactivada. No entanto, recomendamos uma verificação completa do seu computador, imediatamente, após a instalação do programa.

3.2.6. Restringir o acesso ao programa

O Kaspersky Anti-Virus dá-lhe a opção de proteger o programa com uma password, uma vez que várias pessoas poderão usar o mesmo computador e uma vez que os programas maliciosos podem desactivar a protecção. A utilização de uma password pode proteger o programa de tentativas não autorizadas para desactivar a protecção ou alterar as definições.

Para activar a protecção por password, seleccione ☑ **Activar protecção por password** e complete os campos **Password** e **Confirmar password**.

Especifique a área à qual pretende aplicar a protecção por password:

◉ **Todas as operações (excepto notificações de objectos perigosos)**. Requer password se o utilizador tentar executar alguma acção com o programa, excepto nas respostas à notificação da detecção de ficheiros perigosos.

◉ **Operações seleccionadas:**

- ☑ **A guardar definições do programa** – Requer password se o utilizador tentar guardar as alterações às definições do programa.
- ☑ **A sair do programa** – Requer password se o utilizador tentar sair do programa.

☑ **A parar/pausar componentes de protecção ou tarefas de verificação de vírus** – Requer password se o utilizador tentar pausar ou desactivar por completo qualquer componente de protecção ou tarefa de verificação de vírus.

3.2.7. Configurar as definições do Anti-Hacker

O Anti-Hacker é a componente do Kaspersky Anti-Virus para Windows Workstations que protege o seu computador nas redes locais e na Internet. Nesta fase, o Assistente de Configuração pede-lhe para criar uma lista de regras que guiará o Anti-Hacker durante a verificação da actividade de rede do seu computador.

3.2.7.1. Determinar o estado de uma zona de segurança

Nesta fase, o Assistente de Configuração analisa o ambiente de trabalho do seu computador. Com base na sua análise, todo o espaço da rede é repartido em zonas:

Internet – A rede mundial. Nesta zona, o Kaspersky Anti-Virus para Windows Workstations funciona como uma firewall pessoal. Ao fazê-lo, existem regras predefinidas para pacotes e ligações que regulam toda a actividade de rede para garantir o máximo de segurança. Você não pode alterar as definições de protecção quando trabalhar nesta zona, para além de poder activar o Modo Furtivo no seu computador para segurança adicional.

Zonas de segurança – determinadas zonas convencionais que correspondem, muitas vezes, a sub-redes nas quais o seu computador está incluído (isso podem ser sub-redes locais em casa ou no trabalho). Por defeito, estas zonas são zonas com um nível de risco médio quando trabalha com elas. Pode alterar os estados destas zonas, com base no seu grau de confiança em relação a uma determinada sub-rede, e pode configurar regras para filtragem de pacotes e para aplicações.

Todas as zonas detectadas serão apresentadas numa lista. Cada uma delas é apresentada com uma descrição, o seu endereço, a máscara de sub-rede e o estado, através do qual uma qualquer actividade de rede será permitida ou bloqueada pelo Anti-Hacker.

- **Internet**. Por defeito, este é o estado atribuído à Internet, visto que quando você acede à Internet, o seu computador está sujeito a todos os tipos de ameaças possíveis. Este estado é também recomendado para redes que não estão protegidas por nenhum programa de anti-vírus, firewalls, filtros, etc. Quando selecciona este estado, o programa garante segurança máxima enquanto utiliza esta zona, especificamente:

    - Bloqueia qualquer actividade de rede NetBios no âmbito da sub-rede.

    - Bloqueia regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede.

  Mesmo que tenha criado uma pasta partilhada, a informação contida na mesma não será disponibilizada a utilizadores de sub-redes com este estado. Para além disso, se este estado for seleccionado para uma determinada sub-rede, você não pode aceder a ficheiros e impressoras desta sub-rede.

- **Rede Local**. O programa atribui este estado à maioria das zonas de segurança detectadas na análise do ambiente de rede do seu computador, com excepção da Internet. Recomenda-se que aplique este estado a zonas com um factor de risco médio (por exemplo, Redes de Área Local de empresas). Se seleccionar este estado, o programa dá permissão a:

    - qualquer actividade de rede NetBios no âmbito da sub-rede

    - regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede

  Seleccione este estado se desejar conceder acesso a certas pastas no seu computador, mas bloquear qualquer outra actividade exterior.

- **Confiável (permitir todas as ligações).** Este estado é atribuído a redes que sinta que são absolutamente seguras e nas quais o seu computador não está sujeito a ataques e tentativas para aceder aos seus dados, quando ligado a essas redes. Quando utiliza este tipo de rede, é permitida toda a actividade de rede. Mesmo se tiver seleccionado a **Protecção Máxima** e tiver criado regras de bloqueio, estas não funcionarão nos computadores remotos de uma rede confiável.

Poderá utilizar o *Modo Furtivo* para uma segurança acrescida quando utilizar redes classificadas como **Internet**. Esta funcionalidade apenas permite as actividades de rede que sejam iniciadas a partir do seu computador. Isto significa que o seu computador se torna invisível em relação ao que o rodeia. Este modo não afecta a performance do seu computador na Internet.

Não recomendamos o uso do Modo Furtivo se o computador estiver a ser usado como servidor (por exemplo, um servidor de e-mail ou HTTP). Caso contrário, os computadores que se ligam ao servidor não conseguirão vê-lo como estando ligado.

Para alterar o estado de uma zona ou para activar/desactivar o **Modo Furtivo**, seleccione-a a partir da lista e utilize as ligações apropriadas na caixa de **Descrição da regra**, que surge por baixo da lista. Pode executar tarefas similares e editar endereços e máscaras de sub-rede na janela **Propriedades da Zona**, janela essa que poderá abrir se clicar em **Editar**.

Pode adicionar uma nova zona à lista enquanto a visualiza. Para o fazer, clique em **Actualizar**. O Anti-Hacker procurará zonas disponíveis, e se detectar alguma, o programa pedir-lhe-á para seleccionar um estado para elas. Além disso, poderá adicionar manualmente novas zonas à lista (se ligar o seu computador portátil a uma nova rede, por exemplo). Para o fazer, utilize o botão **Adicionar** e preencha a informação necessária na janela **Propriedades da Zona**.

Para apagar uma rede da lista, clique no botão **Apagar**.

3.2.7.2. Criar uma lista de aplicações de rede

O Anti-Hacker cria uma regra para controlar a actividade de rede de cada uma dessas aplicações. As regras são aplicadas usando modelos para as aplicações comuns que utilizam ligações de rede, modelos criados na Kaspersky Lab e incluídos no software.

Pode visualizar a lista de aplicações de rede e as regras para as mesmas na janela de definições do Anti-Hacker, que poderá abrir clicando em **Aplicações**.

Para maior segurança, poderá desactivar o armazenamento temporário de DNS quando estiver a utilizar recursos da Internet. Esta funcionalidade reduz, drasticamente, o tempo durante o qual o seu computador está ligado ao recurso de Internet necessário. Contudo, esta funcionalidade constitui, ao mesmo tempo, uma vulnerabilidade perigosa e, ao utilizá-la, os atacantes podem criar fugas de dados que não é possível registar através de uma firewall. Por isso, para aumentar o grau de segurança do seu computador, nós recomendamos que desactive esta funcionalidade, que permite guardar a informação sobre nomes de domínios na memória temporária.

3.2.8. Finalizar o Assistente de Configuração

A última janela do Assistente irá perguntar-lhe se deseja reiniciar o computador para concluir a instalação do programa. Tem de reiniciar o seu computador, para que os controladores do Kaspersky Anti-virus para Windows Workstations sejam correctamente registados.

Algumas componentes do programa não funcionarão até que você reinicie o computador.

3.3. Instalar o programa a partir da linha de comandos

Para instalar o Kaspersky Anti-virus 6.0 para Windows Workstations, digite o seguinte na linha de comandos:

```
msiexec / i <package_name>
```

O Assistente de Instalação iniciar-se-á (ver 3.1 na pág. 34). Quando o programa estiver instalado, você tem que reiniciar o computador.

Para instalar a aplicação de forma não interactiva (sem executar o Assistente de Instalação), digite:

```
msiexec /i <package_name> /qn
```

Esta opção implicará que você reinicie, manualmente, a sua máquina depois da instalação estar concluída. Para reiniciar de forma automática a partir da linha de comandos, digite:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Por favor, tenha em consideração que a reinicialização automática ocorrerá no modo não interactivo (utilizando a chave /qn).

Para instalar a aplicação com uma password de desinstalação, digite:

msiexec /i <package_name> KLUNINSTPASSWD=******, quando efectuar uma instalação interactiva;

msiexec /i <package_name> KLUNINSTPASSWD=****** /qn, quando efectuar uma instalação não interactiva sem reiniciar o sistema;

`msiexec /i <package_name> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, quando efectuar uma instalação não interactiva sem reiniciar o sistema com reinicialização do sistema;

Se instalar o Kaspersky Anti-Virus no modo não interactivo, você pode aceder ao ficheiro *setup.ini*, que contém as definições gerais para a instalação da aplicação (ver A.4 na pág. 334), ao ficheiro de configuração *install.cfg* (ver 18.8 na pág. 301) e ao ficheiro da chave de licença. Tenha em atenção que estes ficheiros devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus.

3.4. Procedimento para instalar o Objecto de Política de Grupo

Esta função é suportada em computadores com o Microsoft Windows 2000 ou superior.

Ao utilizar o **Editor de Objectos de Política de Grupo**, você pode instalar, actualizar e desinstalar o Kaspersky Anti-Virus em estações de trabalho empresariais no âmbito do domínio, sem utilizar o Kaspersky Administration Kit.

3.4.1. Instalar o programa

Para instalar o Kaspersky Anti-Virus:

1. Crie uma pasta partilhada no computador que é o controlador do domínio e copie o pacote de instalação *.msi* do Kaspersky Anti-Virus para essa mesma pasta.

   Também pode copiar o ficheiro *setup.ini*, que contém as definições gerais para a instalação da aplicação (ver A.4 na pág. 334), o ficheiro de configuração *install.cfg* (ver 18.7 na pág. 300) e o ficheiro da chave de licença.

2. Abra o **Editor de Objectos de Política de Grupo** via MMC (para mais informação detalhada sobre a utilização do Objecto de Política de Grupo, consulte a ajuda no Microsoft Windows Server).

3. Crie um novo pacote. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo/ Configuração do Computador/ Definições do Software/ Instalação do Software** e use o comando **Novo**/ **Pacote** a partir do menu de contexto.

Na janela que se abre, especifique o caminho para a pasta partilhada que contém o programa de instalação Anti-Virus (ver 1). Seleccione **Atribuir** a partir da caixa de diálogo **Seleccionar Método de Instalação** e clique em **OK**.

A política de grupo será implementada em cada estação de trabalho na próxima vez que o computador for registado no domínio. O Kaspersky Anti-Virus será então instalado em todos os computadores.

3.4.2. Actualizar o programa

Para actualizar o Kaspersky Anti-Virus:

1. Copie o pacote de instalação que contém a actualização do Kaspersky Anti-Virus no formato *.msi* para a pasta partilhada.
2. Abra o **Editor de Objectos de Política de Grupo** e crie um novo pacote utilizando os passos acima mencionados.
3. Seleccione o novo pacote e seleccione o comando **Propriedades,** a partir do menu de contexto. Na janela de propriedades de pacote, aceda ao separador **Actualizações** e especifique o pacote que contém o programa de instalação para a versão anterior do Kaspersky Anti-Virus. Para instalar a actualização do Kaspersky Anti-Virus e manter as suas definições de protecção, seleccione uma variante da actualização da versão anterior.

A política de grupo será implementada em cada estação de trabalho na próxima vez que o computador for registado no domínio.

Note que o Kaspersky Anti-Virus em computadores com o Microsoft Windows 2000 Professional não pode ser actualizado utilizando o Editor de Objectos de Política de Grupo.

3.4.3. Desinstalar o programa

Para desinstalar o Kaspersky Anti-Virus:

1. Abra o **Editor de Objectos de Política de Grupo**.
2. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo/ Configuração do Computador/ Definições do Software/ Instalação do Software**.

   Seleccione o pacote do Kaspersky Anti-Virus na lista. Abra o menu de contexto e seleccione o comando **Todas as Tarefas/ Remover**.

Na caixa de diálogo **Remover Software**, seleccione a opção **Desinstalar imediatamente o software dos utilizadores e dos computadores** para que o Kaspersky Anti-Virus seja desinstalado da próxima vez que o computador reiniciar.

3.5. Actualizar da versão 5.0 para a versão 6.0

Se o Kaspersky Anti-Virus 5.0 para Windows Workstations estiver instalado no seu computador, você pode actualizá-lo para o Kaspersky Anti-Virus 6.0 para Windows Workstations.

Depois de iniciar o programa de instalação do Kaspersky Anti-Virus 6.0, ser-lhe-á dada a escolhia de primeiro desinstalar a versão 5.0 já instalada. Quando o processo de desinstalação estiver concluído, tem de reiniciar o seu computador e depois começará então a instalação da versão 6.0.

Aviso!

Se estiver a actualizar o Kaspersky Anti-virus 5.0 para a versão 6.0, a partir de uma pasta de rede protegida por password, a versão 5.0 será desinstalada e o computador será reiniciado, sem instalar depois a versão 6.0 da aplicação. Isto acontece porque o programa de instalação não tem privilégios de acesso à pasta de rede. Para resolver este problema, só deve executar o programa de instalação a partir de uma pasta local.

CAPÍTULO 4. INTERFACE DO PROGRAMA

O Kaspersky Anti-virus para Windows Workstations possui uma interface directa, fácil de utilizar. Este capítulo tratará das suas características básicas:

- Ícone de bandeja do sistema (ver 4.1 na pág. 52)
- Menu de contexto (ver 4.2 na pág. 53)
- Janela principal (ver 4.3 na pág. 55)
- Janela de definições do programa (ver 4.4 na pág. 57)

Para além da interface principal do programa, existem extensões para as seguintes aplicações:

- Microsoft Office Outlook – verificações de vírus (ver 8.2.2 na pág. 111) e verificações de spam (ver 13.3.8 na pág. 197)
- Microsoft Outlook Express (Programa de e-mail do Windows) (ver 13.3.9 na pág. 200)
- The Bat! – verificações de vírus (ver 8.2.3 na pág. 113) e verificações de spam (ver 13.3.10 na pág. 202)
- Microsoft Internet Explorer (ver Capítulo 11 na pág. 143)
- Microsoft Windows Explorer (ver 14.2 na pág. 205)

As extensões aumentam as funcionalidades destes programas, permitindo gerir e configurar o Kaspersky Anti-virus para Windows Workstations, a partir das suas próprias interfaces.

4.1. Ícone de bandeja do sistema

Logo após a instalação do Kaspersky Anti-virus para Windows Workstations, surgirá um ícone para o mesmo na bandeja do sistema.

O ícone é uma espécie de indicador para as operações do Kaspersky Anti-virus para Windows Workstations. Reflecte o estado da protecção e mostra algumas das funções básicas executadas pelo programa.

Se o ícone estiver activo (a cores), significa que o computador está protegido. Se o ícone estiver inactivo (a preto e branco), significa que a sua protecção está totalmente parada ou que várias componentes de protecção (ver 2.2.1 na pág. 26) estão desactivadas.

O ícone do Kaspersky Anti-virus para Windows Workstations altera-se em função da operação que está a ser executada:

	está a ser verificado um e-mail.
	está a ser verificado um script.
	está a ser verificado um ficheiro que você ou algum programa está a abrir, a guardar ou a executar.
	As assinaturas de vírus e ameaças do Kaspersky Anti-virus para Windows Workstations e os módulos do programa estão a ser actualizados.
	Ocorreu um erro nalguma componente do Kaspersky Anti-virus.

O ícone também permite o acesso aos elementos centrais da interface do programa: o menu de contexto (ver 4.2 na pág. 53) e a janela principal (ver 4.3 na pág. 55).

Para abrir o menu de contexto, clique sobre o ícone do programa com o botão direito do rato.

Para abrir a janela principal do Kaspersky Anti-virus para Windows Workstations na secção Protecção (este é, por defeito, o primeiro ecrã que aparece quando abre o programa), duas vezes sobre o ícone do programa. Se clicar uma vez, a janela principal abre-se na secção que estava activa da última vez que fechou a janela.

4.2. Menu de contexto

Pode executar tarefas de protecção básicas a partir do menu de contexto (ver Figura 1).

O menu do Kaspersky Anti-virus para Windows Workstations contém os seguintes itens:

Verificar o Meu Computador – Inicia uma verificação completa do seu computador quanto à existência de objectos perigosos. Serão verificados os ficheiros existentes em todas as unidades, incluindo meios de armazenamento removíveis.

Verificação de vírus... – selecciona objectos e inicia a verificação desses objectos quanto à existência de vírus. Por defeito, a lista contém alguns ficheiros, como por exemplo a pasta **Os Meus Documentos**, a pasta

de inicialização, as bases de dados de e-mail, todas as unidades do seu computador, etc. Pode adicionar objectos à lista, seleccionar ficheiros a serem verificados e iniciar verificações de vírus.

Figura 1. O menu de contexto

Actualizar – transfere actualizações dos módulos do programa e assinaturas de ameaças do Kaspersky Anti-virus e instala-as no seu computador.

Monitor de Rede – Permite ver a lista das ligações de rede, portas abertas e o tráfego.

Activar... – activa o programa. Tem que activar a sua versão do Kaspersky Anti-Virus para obter o estatuto de utilizador registado que lhe dá acesso à funcionalidade completa da aplicação e ao Suporte Técnico. Este item do menu apenas está disponível se o programa não estiver activado.

Definições... – Permite ver e configurar as definições do Kaspersky Anti-virus para Windows Workstations.

Abrir o Kaspersky Anti-Virus – abre a janela principal do programa (ver 4.3 na pág. 55).

Parar Protecção – activa ou desactiva, temporariamente, as componentes de protecção (ver 2.2.1 na pág. 26). Este item do menu não afecta as actualizações do programa ou tarefas de verificação de vírus.

Sair – fecha o Kaspersky Anti-virus para Windows Workstations (quando esta opção é seleccionada, a aplicação será descarregada da memória RAM do computador).

Se estiver a decorrer uma tarefa de pesquisa de vírus, o seu nome será apresentado no menu de contexto com um indicador de progresso percentual. Ao seleccionar a tarefa, você pode aceder à janela de relatório para ver os actuais resultados de desempenho.

4.3. Janela principal do programa

A janela principal do Kaspersky Anti-virus para Windows Workstations (ver Figura 2) pode ser dividida em duas partes:

- a parte esquerda da janela, o painel de navegação, guia-o rápida e facilmente até qualquer componente, tarefa de verificação de vírus e de actualização ou funcionalidades do menu de ajuda do programa;
- a parte direita da janela, o painel de informação, contém informação sobre a componente de protecção seleccionada na parte esquerda da janela e apresenta as definições para cada uma delas, oferecendo-lhe ferramentas para executar as nossas verificações de vírus, trabalhar com ficheiros em quarentena e cópias de segurança, gerir chaves de licença, etc.

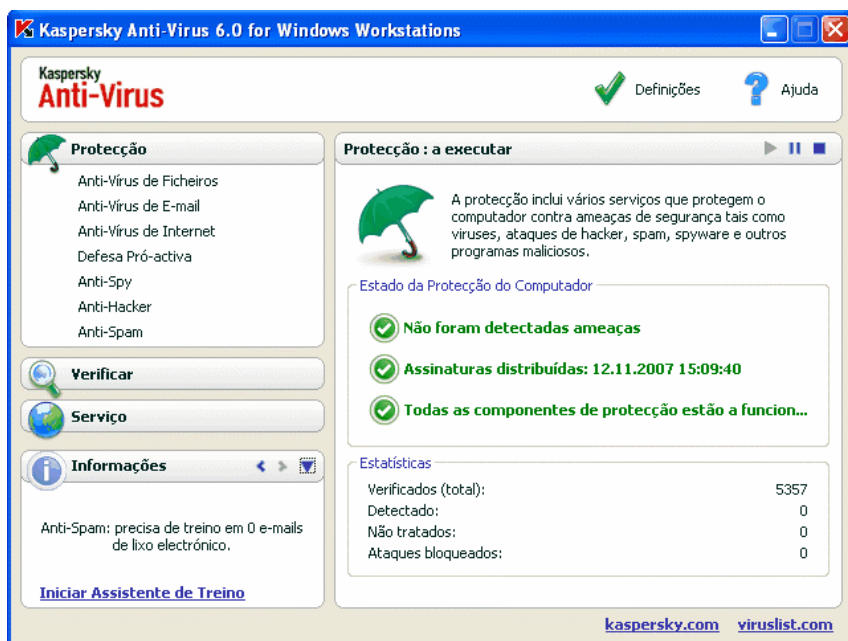
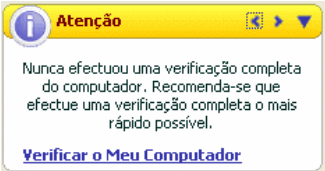



Figura 2. Janela principal do Kaspersky Anti-virus para Windows Workstations

Depois de seleccionar uma secção na parte esquerda da janela, encontrará informação na parte direita que corresponde à sua selecção.

Examinaremos agora, em maior detalhe, elementos existentes no painel de navegação da janela principal.

Secção da Janela Principal	Objectivo
Esta janela serve sobretudo para o informar sobre o estado da protecção do seu computador. A secção **Protecção** está concebida exactamente para isso. Protecção Anti-Vírus de Ficheiros Anti-Vírus de E-mail Anti-Vírus de Internet Defesa Pró-activa Anti-Spy Anti-Hacker Anti-Spam	Para ver informação geral sobre o funcionamento do Kaspersky Anti-Virus, rever as estatísticas gerais do funcionamento do programa e certificar-se de que todas as componentes de protecção estão a funcionar correctamente, seleccione a secção **Protecção** no painel de navegação. Aqui também pode activar/desactivar as componentes de protecção. Para visualizar as estatísticas e definições para uma componente de protecção específica, apenas precisa de seleccionar o nome da componente, acerca da qual deseja obter informações, na secção **Protecção**.
Para verificar o seu computador quanto à existência de ficheiros ou programas maliciosos, utilize a secção especial **Verificar** na janela principal. 	Esta secção contém uma lista de objectos que pode verificar quanto à existência de vírus. As tarefas mais comuns e importantes estão definidas e incluídas na secção. Estas incluem tarefas de verificação de vírus para as áreas críticas, objectos de inicialização e uma verificação completa do computador.
A secção **Serviço** inclui funcionalidades adicionais do Kaspersky Anti-virus para Windows Workstations. 	Aqui poderá actualizar o programa, visualizar relatórios sobre o desempenho de qualquer componentes ou tarefas do Kaspersky Anti-virus para Windows Workstations, trabalhar com, objectos em quarentena, e cópias de segurança, rever informação de suporte técnico, criar um disco de recuperação e gerir chaves de licença.

Secção da Janela Principal	**Objectivo**
A secção **Comentários e Dicas** acompanha-o durante a utilização do programa.	Esta secção oferece dicas sobre como aumentar o nível de protecção do seu computador. Também vai encontrar comentários acerca do desempenho corrente da aplicação e as suas definições. Se utilizar as ligações apresentadas nesta secção, pode facilmente executar as acções recomendadas para uma secção em particular ou ver informação mais detalhada.

Cada elemento do painel de navegação é acompanhado por um menu de contexto especial. Desse modo, o menu contém pontos para a protecção, componentes e ferramentas, que ajudam o utilizador a configurá-las e geri-las mais rapidamente, e ver relatórios. Existe um item de menu adicional para tarefas de verificação de vírus e de actualização que você pode utilizar para criar a sua própria tarefa com base numa tarefa seleccionada.

Pode mudar a aparência do programa, criando e utilizando os seus próprios gráficos e esquemas de cores.

4.4. Janela de definições do programa

Pode abrir a janela de opções do Kaspersky Anti-virus para Windows Workstations a partir da janela principal (ver 4.3 na pág. 55). Para o fazer, clique em Definições na parte superior dessa janela.

A janela de definições (ver Figura 3) é semelhante à janela principal, em termos de disposição:

- a parte esquerda da janela dá-lhe acesso rápido e fácil às definições do Anti-vírus de Ficheiros, das tarefas de procura de vírus e de actualização, assim como das ferramentas do programa;
- a parte direita da janela contém uma lista de definições para a componente, tarefa, etc. seleccionada na parte esquerda da janela.

Quando selecciona uma determinada secção, componente ou tarefa na parte esquerda da janela de definições, a parte direita apresentará as definições básicas para a mesma. Para configurar definições avançadas, pode abrir um

segundo e terceiro nível de janelas de definições. Encontrará uma descrição detalhada das opções do programa nas secções aqui presentes.

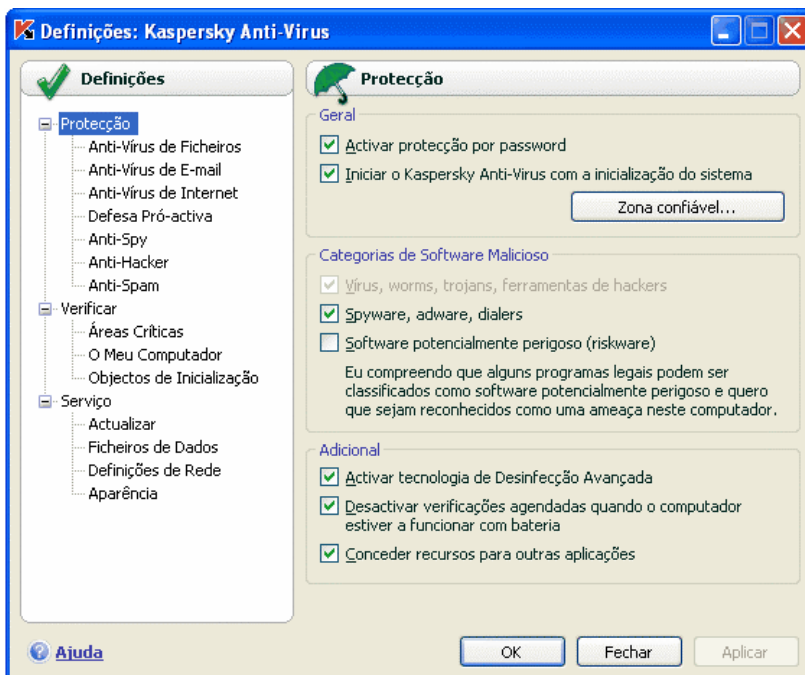



Figura 3. Janela de definições do Kaspersky Anti-virus para Windows Workstations

CAPÍTULO 5. COMEÇAR

Um dos principais objectivos dos especialistas da Kaspersky Lab, ao conceber o Kaspersky Anti-virus para Windows Workstations, foi o de fornecer a configuração óptima para todas as opções do programa. Isso permite que um utilizador, com qualquer nível de conhecimentos informáticos, possa proteger o seu computador logo após a instalação, sem necessitar de despender horas com as definições.

Contudo, os detalhes de configuração para o seu computador ou os trabalhos que realiza com o mesmo podem ter as suas próprias especificidades. Por isso, recomendamos que faça uma configuração preliminar para conseguir a abordagem mais flexível e personalizada da protecção do seu computador.

Para a conveniência do utilizador, reunimos as etapas de configuração preliminar numa interface: o Assistente de Configuração Inicial (ver 3.2 na pág. 38) que se inicia assim que o programa é instalado. Ao seguir as instruções do Assistente, você pode activar o programa, configurar definições para as actualizações e verificações de vírus, proteger o acesso ao programa com uma password e configurar o Anti-Hacker, de forma a que este se adapte às propriedades da sua rede.

Depois de completar a instalação e iniciar o programa, recomendamos que siga os seguintes passos:

- Verifique o estado actual de protecção (ver 5.1 na pág. 59) para ter a certeza de que o Kaspersky Anti-virus para Windows Workstations está a funcionar com o nível adequado.
- Treine o Anti-Spam (ver 5.5 na pág. 68) utilizando os seus e-mails.
- Actualize o programa (ver 5.6 na pág. 69) (se o Assistente de Configuração não o tiver feito automaticamente após a instalação do programa).
- Verifique o computador (ver 5.2 na pág. 65) quanto à existência de vírus.

5.1. Qual o estado da protecção que o computador tem?

As informações compostas sobre a protecção do seu computador são fornecidas na janela principal do Kaspersky Anti-virus na secção **Protecção**. O *actual estado de protecção* do computador e as *estatísticas gerais de funcionamento* do programa são apresentadas aqui.

O **estado de protecção** mostra o actual estado de protecção do seu computador utilizando indicadores especiais (ver 5.1.1 na pág. 60). As estatísticas (ver 5.1.2 na pág. 63) analisam a actual sessão do programa.

5.1.1. Indicadores de protecção

O **estado de protecção do computador** é determinado por três indicadores que reflectem o grau de protecção do seu computador naquela altura e que o informam sobre problemas nas definições e desempenho do programa.

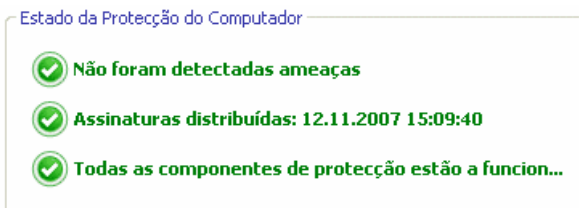



Figura 4. Indicadores que reflectem o estado de protecção do programa

Cada indicador pode assumir três possíveis aparências:

– O *indicador é de natureza indicativa*; permite-lhe saber que a protecção do seu computador está no nível adequado e que não foram detectados problemas nas definições e desempenho do programa ou das suas componentes.

– O *indicador direcciona a sua atenção para vários desvios* de desempenho do Kaspersky Anti-virus para Windows Workstations, em relação ao nível de desempenho adequado, o que poderá afectar a segurança da informação. Tenha em atenção as recomendações dos especialistas da Kaspersky Lab. As acções recomendadas são apresentadas como ligações.

– O *indicador reflecte situações críticas* na protecção do seu computador. Siga cuidadosamente as instruções. Elas foram concebidas para uma melhor protecção do seu computador. As acções recomendadas são apresentadas como ligações.

Examinaremos agora, mais detalhadamente, os indicadores de protecção e as situações que cada um deles indica.

O primeiro indicador reflecte a situação com ficheiros e programas maliciosos no seu computador. O indicador assume um dos seguintes valores:

	Não foram detectadas ameaças O Kaspersky Anti-virus para Windows Workstations não detectou qualquer ficheiro ou programa perigoso no seu computador.
	Foram neutralizadas todas as ameaças O Kaspersky Anti-virus para Windows Workstations tratou todos os ficheiros e programas infectados com vírus e apagou aqueles que não podiam ser tratados.
	Foram detectadas ameaças O seu computador está em risco de infecção. O Kaspersky Anti-virus detectou programas maliciosos (vírus, Trojans, worms, etc.) que têm que ser neutralizados. Para o fazer, utilize a ligação Neutralizar Todos. Clique na ligação Detalhes para ver informação mais detalhada acerca dos objectos maliciosos.

O segundo indicador reflecte a eficácia da protecção do seu computador naquele momento. O indicador assume um dos seguintes valores:

	Assinaturas distribuídas (data, tempo) A aplicação e as assinaturas de ameaças do Kaspersky Anti-virus para Windows Workstations são as versões mais recentes.
	Assinaturas desactualizadas Os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-virus para Windows Workstations já não são actualizados há uma série de dias. Você está correr o risco de infectar o seu computador com novos programas maliciosos que apareceram desde que actualizou o programa pela última vez. Recomendamos que actualize o Kaspersky Anti-virus para Windows Workstations. Para o fazer, utilize a ligação Actualizar.
	As assinaturas estão parcialmente corrompidas Os ficheiros das assinaturas de ameaça estão parcialmente danificados. Se tal acontecer, recomenda-se que actualize novamente o programa. Se encontrar a mesma mensagem de erro novamente, contacte o Serviço de Suporte Técnico da Kaspersky Lab.

	Por favor, reinicie o seu computador Para que o programa corra correctamente, deverá reiniciar os seu computador. Guarde e feche todos os ficheiros em que estiver a trabalhar e utilize a ligação Reiniciar o computador.
	As actualizações do programa estão desactivadas O serviço de actualização das assinaturas de ameaças e dos módulos do programa está desactivado. Para manter a protecção, em tempo real, recomendamos que active as actualizações.
	As assinaturas estão obsoletas O Kaspersky Anti-virus para Windows Workstations já não é actualizado há algum tempo. Você está a colocar em risco os dados do seu computador. Actualize o programa o mais rapidamente possível. Para o fazer, utilize a ligação Actualizar.
	As assinaturas estão corrompidas Os ficheiros das assinaturas de ameaça estão total ou parcialmente danificados. Se tal acontecer, recomenda-se que actualize novamente o programa. Se encontrar a mesma mensagem de erro novamente, contacte o Serviço de Suporte Técnico da Kaspersky Lab.

O terceiro indicador reflecte o actual estado de funcionamento do programa. O indicador assume um dos seguintes valores:

	Todas as componentes de protecção estão a funcionar O Kaspersky Anti-virus para Windows Workstations está proteger o seu computador em todos os canais através dos quais os programas maliciosos poderão penetrar. Todas as componentes de protecção estão activadas.
	A protecção não está instalada Quando o Kaspersky Anti-virus para Windows Workstations foi instalado, nenhuma das componentes de monitorização foi instalada. Isso significa que apenas pode executar verificações de vírus. Para conseguir máxima segurança, deve instalar as componentes de protecção no seu computador.

	Todas as componentes de protecção estão pausadas A componente de protecção foi pausada. Para restaurar a componente, seleccione **Retomar Protecção** a partir do menu de contexto, clicando no ícone da bandeja do sistema.
	Algumas componentes de protecção estão desactivadas Uma ou mais componentes de protecção foram paradas. Isso pode-se tornar a causa de uma infecção no seu computador e a perda de dados. Recomendamos vivamente que active a protecção. Para o fazer, seleccione uma componente inactiva a partir da lista e clique em .
	Todas as componentes de protecção estão desactivadas A protecção está completamente desactivada. Não existem componentes de a funcionar. Para restaurar as componentes, seleccione **Retomar Protecção** a partir do menu de contexto, clicando no ícone da bandeja do sistema.
	Algumas componentes de protecção falharam A componente do Kaspersky Anti-virus para Windows Workstations produziram erros internos. Se isso ocorrer, recomenda-se que active a componente ou reinicie o computador (é possível que os controladores da componente tenham que ser registados após terem sido actualizados).

5.1.2. Estado das componentes do Kaspersky Anti-Virus para Windows Workstations

Para descobrir como é que o Kaspersky Anti-virus para Windows Workstations está a proteger o seu sistema de ficheiros, correio electrónico, tráfego HTTP e outras áreas onde os programas perigosos podem penetrar no seu computador ou para visualizar a tarefa de análise de vírus ou o progresso na actualização das assinaturas de ameaça, bastará abrir a secção correspondente da janela principal do programa.

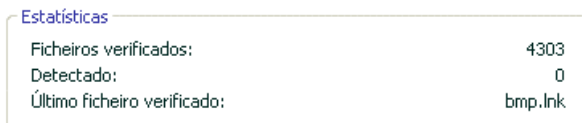
Por exemplo, para visualizar o estado actual do **Anti-Vírus de Ficheiros**, seleccione o Anti-vírus de Ficheiros na parte esquerda da janela principal e para ver se está protegido contra novos tipos de vírus, seleccione a **Defesa Pró-**

activa. A parte direita da janela exibirá informação completa sobre o funcionamento das componentes.

Para as componentes de protecção, está dividida na **barra de estado**, a caixa **Estado (Definições** para a análise de vírus e tarefas de actualização) e a caixa **Estatísticas**.

Para o Anti-vírus de Ficheiros a *barra de estado* aparece da seguinte forma:

- *Anti-vírus de Ficheiros* : *a executar* – a protecção de ficheiros está activa para o nível seleccionado (ver 7.1 na pág. 93).
- *Anti-vírus de Ficheiros : pausado* – O Anti-vírus de Ficheiros está desactivado durante um determinado período de tempo. A componente retomará as operações, automaticamente, depois do período definido ter terminado ou depois de reiniciar o programa. Também pode retomar, manualmente, a protecção de ficheiros, clicando no botão na barra de estado.
- *Anti-vírus de Ficheiros* : *parado* – a componente foi parada pelo utilizador. Pode activar a protecção de ficheiros. Para o fazer, clique no botão na barra de estado.
- *Anti-vírus de Ficheiros: não está a funcionar* – Por alguma razão, a protecção de ficheiros não está disponível.
- *Anti-vírus de Ficheiros: desactivado (erro)* – componente encontrou um erro.

  Se uma componente encontrar um erro, tente reiniciá-la. Se o reinício resultar num erro, reveja o relatório da componente que pode conter a razão para a falha. Se não for capaz de resolver o problema por si só, guarde o relatório da componente num ficheiro, utilizando **Acções → Guardar como** e contacte o Suporte Técnico da Kaspersky Lab.

Se a componente tiver vários módulos, a secção **Estado** terá informação sobre qual deles está activado. Para as componentes que não possuem módulos individuais, é exibido o seu estado, nível de segurança e, para algumas componentes, a acção executada em resposta a programas perigosos.

Não existe a caixa de **Estado** para as verificações de vírus ou tarefas de actualização. O nível de segurança, a acção aplicada a programas perigosos para as tarefas de verificação de vírus e o modo de funcionamento para as actualizações estão enumeradas na caixa **Definições**.

A caixa **Estatísticas** contém informação sobre o funcionamento das componentes de protecção, actualizações ou tarefas de verificação de vírus.

5.1.3. Estatísticas de funcionamento do programa

As **estatísticas do programa** podem ser encontradas na caixa **Estatísticas** da secção **Protecção** da janela principal do programa e exibem informação geral sobre a protecção do computador, guardadas desde que instalou o Kaspersky Anti-virus para Windows Workstations.

Figura 5. Caixa das estatísticas gerais do programa

Pode clicar com o botão esquerdo do rato em qualquer sítio da caixa para visualizar um relatório com informação detalhada. Os Separadores mostram:

- Informação sobre os objectos encontrados (ver 17.3.2 na pág. 249) e o estado que lhes foi atribuído
- Registo de eventos (ver 17.3.3 na pág. 250)
- Estatísticas gerais de verificação (ver 17.3.4 na pág. 252) para o seu computador
- Definições de funcionamento do programa (ver 17.3.5 na pág. 252)

5.2. Como verificar a existência de vírus no seu computador

Depois da instalação, o programa informá-lo-á, através de um aviso especial na parte inferior esquerda da janela da aplicação, de que o computador ainda não foi verificado e recomendará que verifique, imediatamente, a existência de vírus no mesmo.

O Kaspersky Anti-virus para Windows Workstations inclui uma tarefa predefinida para a verificação de vírus no computador. Esta tarefa está incluída na janela principal do programa na secção **Verificar**.

Após seleccionar a tarefa intitulada **Áreas Críticas**, poderá ver as estatísticas da última verificação do computador e as definições da tarefa: estatísticas para a verificação mais recente destas áreas; definições de tarefas; o nível de

protecção seleccionado e que acções serão tomadas em relação às ameaças de segurança. Aqui também pode seleccionar as áreas críticas que deseja verificar e analisar, de imediato, essas áreas.

Para verificar as áreas críticas, quanto à existência de programas maliciosos,

1. Abra a janela principal do programa e seleccione a tarefa **Áreas Críticas** na secção **Verificar**.
2. Clique no botão **Verificar**.

Como resultado, o programa começará a verificar o seu computador e os detalhes serão apresentados numa janela especial. Quando clicar no botão **Fechar,** a janela com informações sobre o progresso da verificação será ocultada, mas isso não interromperá a verificação.

5.3. Como verificar as áreas críticas do computador

Estas são áreas no seu computador que são críticas do ponto de vista da segurança. Estas são os alvos de programas maliciosos, que têm como objectivo danificar o hardware do seu computador, incluindo o seu sistema operativo, o processador, a memória, etc.

É extremamente importante garantir a segurança das áreas críticas do seu computador, para assegurar que o mesmo continua a funcionar. Para sua conveniência, programámos antecipadamente uma tarefa de verificação de vírus especificamente para estas áreas. Esta tarefa está incluída na janela principal do programa na secção **Verificar**.

Depois de seleccionar a tarefa intitulada **Áreas Críticas**, poderá ver as estatísticas para a última verificação do computador e as definições da tarefa: que nível de protecção foi seleccionado e quais as acções que são aplicadas em relação a ameaças de segurança. Aqui quais as áreas críticas que pretende verificar e iniciar, de imediato, uma verificação de vírus nas áreas seleccionadas.

Para verificar as áreas críticas do seu computador, quanto à existência de programas maliciosos,

1. Abra a janela principal do programa e seleccione a tarefa **Áreas Críticas** na secção **Verificar**.
2. Clique no botão **Verificar**.

Como resultado, será iniciada uma verificação das áreas seleccionadas e os detalhes serão apresentados numa janela especial. Quando clicar no botão

Fechar, a janela com informações sobre o progresso da verificação será ocultada, mas isso não interromperá a verificação.

5.4. Como verificar a existência de vírus num ficheiro, pasta ou disco

Há situações em que é necessário verificar a existência de vírus em objectos individuais e não em todo o computador. Por exemplo, um dos discos rígidos onde estão localizados os seus programas e jogos, bases de dados de e-mail trazidas do trabalho para casa e ficheiros arquivados que recebeu por e-mail, etc. Você pode seleccionar um objecto para verificação com as ferramentas padrão do Microsoft Windows (por exemplo, na janela do **Explorador** ou na sua **Área de Trabalho**, etc.).

Para analisar um ficheiro,

> Coloque o cursor em cima do nome do ficheiro seleccionado, abra o menu de contexto do Windows, clicando com o botão direito do rato, e seleccione **Verificar Vírus** (ver Figura 6).

Começará a verificação do objecto seleccionado e os detalhes serão apresentados numa janela especial. Quando clicar no botão **Fechar,** a janela com informações sobre o progresso da verificação será ocultada, mas isso não interromperá a verificação.

Figura 6. Verificar um ficheiro seleccionado utilizando o menu de contexto padrão do Windows

5.5. Como treinar o Anti-Spam

Um dos passos, para começar a utilizar o programa, consiste em treinar o Anti-Spam para trabalhar com os seus e-mails e filtrar o lixo electrónico. O Spam são e-mails de lixo electrónico, embora seja muito difícil dizer o que constitui spam para um determinado utilizador. Claro que existem categorias de e-mails que podem ser classificadas como spam com um elevado nível de precisão (por exemplo, envio em massa de e-mails, publicidade, e-mails codificados em Chinês), mas esses mesmos e-mails poderiam fazer parte da caixa de entrada de alguns utilizadores.

Por isso, pedimos-lhe que determine, por si próprio, que e-mails são spam e que e-mails não o são. Depois da instalação, o Kaspersky Anti-Virus para Windows Workstations irá perguntar-lhe se deseja treinar o Anti-Spam para diferenciar entre e-mails de spam e bons e-mails. Você pode fazer isto com botões especiais que são incluídos no seu cliente de e-mail (Microsoft Office Outlook, Microsoft Outlook Express (Programa de E-mail do Windows), The Bat!) ou utilizando o Assistente de Treino.

> Aviso!
>
> Esta versão do Kaspersky Anti-Virus não contém plug-ins do Anti-Spam para o Microsoft Office Outlook com o Microsoft Windows 98.

Para treinar o Anti-Spam com os botões especiais,

1. Abrir o seu cliente de e-mail predefinido no computador (ex. Microsoft Office Outlook). Verá dois botões na barra de ferramentas: **Spam** e **Não-Spam**.
2. Seleccione um e-mail que considera adequado ou um grupo de e-mails que contenha um e-mail adequado e clique em **Não-Spam**. A partir daí, todos os e-mails com origem nos endereços desses e-mails que seleccionou serão sempre processados como não-spam.
3. Seleccione um e-mail que considera spam, um grupo de e-mails ou uma pasta com esses e-mails e clique em **Spam**. O Anti-Spam analisará os conteúdos destes e-mails e, no futuro, todos os e-mails com conteúdos similares serão considerados como spam.

Para treinar o Anti-Spam com o Assistente de Treino,

1. Abra a janela de definições do programa, seleccione a componente **Anti-Spam** na secção **Protecção** e clique no botão **Assistente de Treino**..
2. Siga as instruções do Assistente de Treino do Anti-Spam (ver 13.2.1, pág. 181).

Quando um e-mail chegar à sua caixa de entrada, o Anti-Spam verifica-o quanto aos conteúdos de spam e adiciona uma expressão especial [Spam] à linha de assunto do spam. Você pode configurar uma regra especial para estes e-mails no seu cliente de e-mail, como por exemplo uma regra que apaga estes e-mails ou que os move para uma pasta especial.

5.6. Como actualizar o Programa

A Kaspersky Lab actualiza as assinaturas de ameaças e os módulos internos do Kaspersky Anti-virus para Windows Workstations, utilizando servidores de actualização.

Os *servidores de actualização da Kaspersky Lab* são os sites da Kaspersky Lab onde as actualizações do programa estão armazenadas.

> Aviso!
>
> Necessitará de uma ligação à Internet para actualizar o Kaspersky Anti-virus para Windows Workstations.

O Kaspersky Anti-virus para Windows Workstations verifica, automaticamente, a existência de actualizações nos servidores da Kaspersky Lab. Se o servidor tiver as actualizações mais recentes, o Kaspersky Anti-virus para Windows Workstations irá transferi-las e instalá-las em modo silencioso.

Para actualizar, manualmente, o Kaspersky Anti-virus para Windows Workstations,

seleccione a componente **Actualização** na secção **Serviço** da janela principal do programa e clique no botão **Actualizar agora!** na parte direita da janela.

Como resultado, o Kaspersky Anti-virus para Windows Workstations começará a actualização. Os detalhes do processo serão apresentados numa janela especial.

5.7. O que fazer se a protecção não estiver a funcionar

Se ocorrerem problemas ou erros no funcionamento de qualquer componente de protecção, verifique qual é o estado dessa componente. Se o estado da componente for *não está a funcionar* ou *mau funcionamento*, experimente reiniciar o Kaspersky Anti-virus.

Se o problema não for resolvido depois de reiniciar o programa, recomendamos que corrija erros possíveis, utilizando a função de restauro da aplicação (ver Capítulo 19, pág. 304).

Se o procedimento de restauro da aplicação não ajudar, contacte o Serviço de Suporte Técnico da Kaspersky Lab. Poderá precisar de guardar em ficheiro um relatório sobre o funcionamento da componente ou de toda a aplicação e enviá-lo para a Kaspersky Lab para investigação.

Para guardar o relatório num ficheiro:

1. Seleccione a componente na secção **Protecção** da janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da secção **Estatísticas**.
2. Clique no botão **Guardar como** e, na janela que se abre, especifique o nome do ficheiro para o relatório de funcionamento da componente.

Para guardar um relatório para todas as componentes do Kaspersky Anti-Virus para Windows Workstations de uma só vez (componentes de protecção, tarefas de verificação de vírus, funcionalidades de suporte):

1. Seleccione a componente na secção **Protecção** da janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da secção **Estatísticas**.

   ou

   Clique em Todos os relatórios na janela de relatórios para qualquer componente. Deste modo, o Separador **Relatórios** mostrará uma lista de relatórios para todas as componentes do programa.
2. Clique no botão **Guardar como** e, na janela que se abre, especifique o nome do ficheiro para o relatório de funcionamento da componente.

CAPÍTULO 6. SISTEMA DE GESTÃO DA PROTECÇÃO

O Kaspersky Anti-Virus para Windows Workstations possibilita-lhe a gestão da segurança do computador com multi-tarefas:

- Activar, desactivar e pausar (ver 6.1 na pág. 71) o programa
- Definir os tipos de programas perigosos (ver 6.2 na pág. 76) em relação aos quais o Kaspersky Anti-virus para Windows Workstations protegerá o seu computador
- Criar uma lista de exclusões (ver 6.3 na pág. 77) da protecção
- Criar a sua própria tarefa de verificação de vírus e actualização (ver 6.4 na pág. 87)
- Configurar tarefas de verificação de vírus e actualizações agendadas (ver 6.5 na pág. 88)
- Configurar definições de produtividade (ver 6.6 na pág. 90) para a protecção anti-vírus

6.1. Parar e Retomar a protecção no seu computador

Por definição, o Kaspersky Anti-virus arranca e protege o seu computador durante o tempo em que o utilizar. As palavras *Protegido pelo Kaspersky Anti-virus* no canto superior direito do ecrã indicam-lhe que todas as componentes estão a funcionar (ver 2.2.1 na pág. 25).

Poderá desactivar, total ou parcialmente, a protecção fornecida pelo Kaspersky Anti-virus para Windows Workstations.

Aviso!

A Kaspersky Lab recomenda vivamente que **não desactive a protecção**, já que isso poderia levar a uma infecção no seu computador ou à perda de dados.

Note que neste caso a protecção é abordada no contexto das componentes de protecção. Desactivar ou pausar componentes de protecção não afecta a performance das tarefas de verificação de vírus e das actualizações do programa.

6.1.1. Pausar a protecção

Pausar a protecção significa desactivar, temporariamente, todas as componentes de protecção que monitorizam os ficheiros do seu computador, e-mails de entrada e de saída, scripts executáveis, o comportamento das aplicações, o Anti-Hacker e o Anti-Spam.

Para pausar o funcionamento do Kaspersky Anti-virus para Windows Workstations:

1. Seleccione **Parar protecção** no menu de contexto do programa (ver 4.2 na pág. 53).
2. Na janela **Parar protecção** que se abre (ver Figura 7), seleccione o período de tempo a partir do qual você pretende que a protecção seja activada:
   - **Dentro de <intervalo de tempo>** – a protecção será activada após este período de tempo. Para seleccionar um intervalo de tempo, use o menu suspenso.
   - **Na próxima vez que reiniciar o programa** – a protecção será retomada se abrir o programa a partir do Menu Iniciar ou depois de reiniciar o seu computador (desde que o programa esteja definido para se iniciar quando o computador for ligado (ver 6.1.5 na pág. 75)).
   - **Apenas a pedido do utilizador** – a protecção estará parada até que você a inicie. Para activar a protecção, seleccione **Retomar Protecção** no menu de contexto do programa.

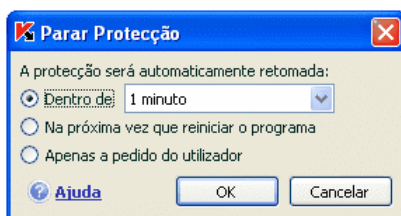



Figura 7. Janela Parar protecção

Dica:

Também pode parar a protecção do seu computador através de um dos seguintes métodos:

- Clique no botão na secção Protecção.
- Seleccione **Sair** no menu de contexto. Neste caso, o programa será descarregado da memória do computador.

Se pausar a protecção, todas as componentes de protecção serão pausadas. Isto é indicado por:

- Nomes inactivos (a cinzento) das componentes desactivadas na secção **Protecção** da janela principal.
- Ícone da bandeja do sistema inactivo (a cinzento).
- O terceiro indicador de protecção (ver 5.1.1 na pág. 60) do seu computador, que mostra que **Todas as componentes de protecção estão pausadas**.

6.1.2. Desactivar a protecção

Parar a protecção significa desactivar completamente as suas componentes. As tarefas de verificação de vírus e actualizações continuarão a funcionar neste modo.

Se a protecção for desactivada por completo, esta apenas pode ser activada através de instrução do utilizador. Em tal caso, as componentes de protecção não são automaticamente activadas depois de reiniciar o sistema ou o programa. Lembre-se que se o Kaspersky Anti-virus para Windows Workstations estiver, de alguma forma, em conflito com outros programas instalados no seu computador, você pode pausar componentes individuais ou criar uma lista de exclusões (ver 6.3 na pág. 77).

Para parar, por completo, a protecção:

1. Abra a janela de definições do Kaspersky Anti-Virus e seleccione a secção **Protecção**.
2. Desmarque a opção **Activar protecção**.

Como resultado da desactivação da protecção, todas as componentes de protecção serão paradas. Isto é indicado por:

- Nomes inactivos (a cinzento) das componentes na secção Protecção da janela principal.

- Ícone da bandeja do sistema inactivo (a cinzento).
- O terceiro indicador de protecção (ver 5.1.1 na pág. 60) no seu computador, que mostra que **Todas as componentes de protecção estão desactivadas**.

6.1.3. Pausar/ desactivar componentes de protecção e tarefas

Existem várias formas de parar uma componente de protecção, as verificações de vírus ou as actualizações. No entanto, antes de o fazer, recomendamos que estabeleça a razão pela qual as deseja parar. É provável que consiga resolver o problema de outra forma, por exemplo, alterando o nível de segurança. Se, por exemplo, estiver a trabalhar com uma base de dados que tem a certeza que não contém vírus, pode simplesmente adicionar os seus ficheiros como uma exclusão (ver 6.3 na pág. 77).

Para suspender as componentes de protecção, tarefas de verificações de vírus e actualizações:

Seleccione a componente ou tarefa na parte esquerda da janela principal e clique no botão na barra de estado.

O estado da componente/tarefa alterar-se-á para ***pausado***. A componente/tarefa será pausada até que a active, clicando no botão .

Quando pausa uma componente ou tarefa, as estatísticas do Kaspersky Anti-Virus para a actual sessão do Kaspersky Anti-virus para Windows Workstations são guardadas e continuam a ser gravadas depois da componente ou tarefa ser reactivada.

Para parar as componentes de protecção, tarefas de verificações de vírus e actualizações:

Clique no botão na barra de estado. Também pode parar a componentes de protecção na janela de definições do programa desmarcando a opção **Activar <nome da componente>** na secção **Geral** para essa componente.

O estado da componente/tarefa passará então para *desactivado* (parado). A componente ou tarefa ficará parado até que o active clicando no botão . Para as tarefas de verificações de vírus e actualizações terá de escolher entre as seguintes opções: continuar a tarefa que foi interrompida ou começá-la de novo.

Quando pára uma componente ou tarefa protecção, todas as estatísticas de trabalhos anteriores são limpas e quando a componente é iniciada, as estatísticas são gravadas por cima, substituindo as anteriores.

6.1.4. Restaurar a protecção no seu computador

Se a dada altura pausou ou desactivou a protecção do seu computador, pode reactivá-la utilizando os seguintes métodos:

- *A partir do menu de contexto*.

  Para o fazer, seleccione **Retomar Protecção.**

- *A partir da Janela Principal do Programa.*

  Para o fazer, clique no botão na barra de estado na secção Protecção na Janela Principal.

O estado da protecção altera-se, de imediato, para ***em execução***. O ícone da bandeja do sistema do programa passa a estar activo (a cores). O terceiro indicador de protecção (ver 5.1.1 na pág. 60) também o informará de que **Todas as componentes de protecção estão activadas**.

6.1.5. Encerrar o programa

Se tiver que encerrar o Kaspersky Anti-virus para Windows Workstations, seleccione **Sair** no menu de contexto do programa (ver 4.2 na pág. 53). A seguir, o programa irá descarregar-se da memória RAM do seu computador, o que significa que o seu computador estará a funcionar desprotegido.

Quando fechar o programa, se estiverem em execução no seu computador as ligações de rede que o programa monitoriza, aparecerá um aviso no ecrã informando que estas ligações serão desactivadas. Isto é necessário para que o programa seja devidamente encerrado. As ligações são automaticamente cortadas após 10 segundos ou se clicar em **Sim**. A maioria das ligações terminadas serão restauradas após um curto período de tempo.

> Note que, quando a ligação for terminada, se você estiver a transferir um ficheiro sem um gestor de transferências, essa transferência de ficheiro será interrompida. Terá que transferir novamente o ficheiro.

Poderá optar por não interromper as ligações, se clicar em **Não** na janela de aviso. Se o fizer, o programa continuará em execução.

Depois de fechar o programa, você pode activar, novamente, a protecção do computador, abrindo o Kaspersky Anti-virus para Windows Workstations (**Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0 para Windows Workstations** → **Kaspersky Anti-Virus 6.0 para Windows Workstations**).

Também poderá retomar, automaticamente, a protecção depois de reiniciar o seu sistema operativo. Para activar esta funcionalidade, seleccione a secção **Protecção** na janela de definições do programa e assinale a opção ☑ **Iniciar o Kaspersky Anti-virus com a inicialização do sistema**.

6.2. Tipos de programas maliciosos a monitorizar

O Kaspersky Anti-virus para Windows Workstations protege o seu computador de vários tipos de programas maliciosos. Sem ter em conta as suas definições, o programa protege sempre o seu computador contra os tipos mais perigosos de programas maliciosos, como vírus, trojans e ferramentas de hackers. Estes programas podem provocar danos significativos no seu computador. Para tornar o seu computador mais seguro, pode aumentar a lista de ameaças que o programa detectará, fazendo-o monitorizar mais tipos de programas perigosos.

Para escolher quais os programas maliciosos, em relação aos quais o Kaspersky Anti-virus para Windows Workstations o irá proteger, seleccione a secção **Protecção** na janela de definições do programa (ver 4.4 na pág. 57).

A caixa **Categorias de Software Malicioso (malware)** contém tipos de ameaças (ver 1.1na pág. 11):

☑ **Vírus, worms, trojans, ferramentas de hackers**. Este grupo reúne as categorias mais comuns e perigosas de programas maliciosos. Este é o nível de segurança mínimo admissível e desactivá-lo aumentaria significativamente a possibilidade do seu computador ser infectado. De acordo com as recomendações dos especialistas da Kaspersky Lab, você não pode remover estes objectos da lista de objectos que o Kaspersky Anti-virus monitoriza.

☑ **Spyware, adware, dialers**. Este grupo reúne software potencialmente perigoso que poderia servir como fonte de perigo.

☑ **Software potencialmente perigoso (riskware).** Este grupo inclui programas que não são maliciosos ou perigosos. Contudo, em determinadas circunstâncias, estes podem ser utilizados para causar danos no seu computador.

Os grupos acima listados incluem a totalidade das ameaças que o programa detecta ao verificar objectos.

Se todos os grupos estiverem seleccionados, o Kaspersky Anti-Virus para Windows Workstations fornece a protecção anti-vírus mais completa possível para o seu computador. Se o segundo e terceiro grupos estiverem desactivados, o programa apenas o protegerá dos programas maliciosos mais comuns. Isto

não inclui programas potencialmente perigosos e outros que possam estar instalados no seu computador e que possam causar danos nos seus ficheiros, roubar o seu dinheiro ou consumir o seu tempo.

A Kaspersky Lab aconselha a não desactivar a monitorização do segundo grupo. Se ocorrer uma situação em que o Kaspersky Anti-virus para Windows Workstations classifica como potencialmente perigoso um programa que você não considera perigoso, recomendamos que crie uma exclusão para o mesmo (ver 6.3na pág. 77).

6.3. Criar uma zona confiável

Uma zona *confiável* é uma lista de objectos, criada pelo utilizador, que o Kaspersky Anti-virus para Windows Workstations não monitoriza. Ou seja, é um conjunto de programas excluídos da protecção.

O utilizador cria uma zona protegida com base nas propriedades dos ficheiros que utiliza e nos programas instalados no seu computador. Você pode precisar de criar uma lista de exclusões se, por exemplo, o Kaspersky Anti-virus para Windows Workstations bloquear o acesso a um objecto ou programa e você tiver a certeza de que o ficheiro ou programa é absolutamente seguro.

Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos, de acordo com o estado que programa atribui aos objectos durante uma verificação).

> Aviso!
>
> Um objecto de exclusão não é sujeito a verificação quando o disco ou pasta onde se encontra é verificado. Contudo, se seleccionar aquele objecto em particular, a regra de exclusão não se aplicará.

Para criar uma lista de exclusões,

1. Abra a janela de definições da aplicação para Windows Workstations e seleccione a secção **Protecção**.
2. Clique no botão **Zona confiável** na secção **Geral.**
3. Configure as regras de exclusão para objectos e crie uma lista de aplicações confiáveis na janela que se abre (ver Figura 8).

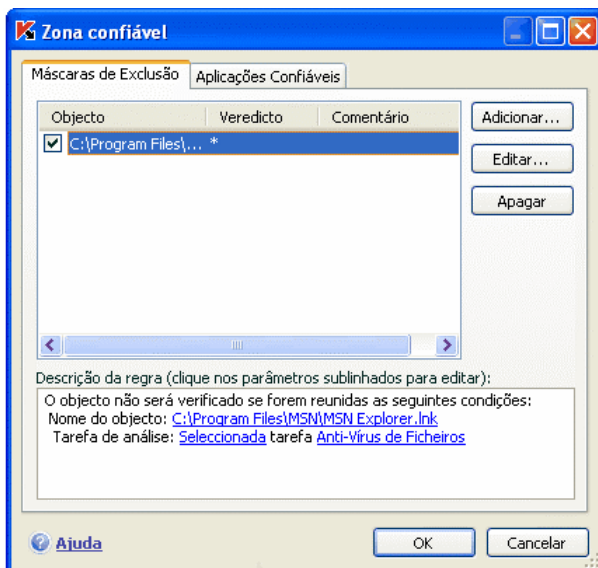



Figura 8. Criar uma zona confiável

6.3.1. Regras de exclusão

As regras de exclusão são conjuntos de condições que o Kaspersky Anti-virus para Windows Workstations usa para saber quando não deve verificar um objecto.

Você pode excluir da verificação os ficheiros de determinados formatos, utilizando uma máscara de ficheiro ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objectos, de acordo com o seu veredicto.

O *veredicto* é o estado que o Kaspersky Anti-virus para Windows Workstations atribui a um objecto durante a verificação. Um veredicto é atribuído com base na classificação de programas maliciosos e potencialmente perigosos encontrados na Enciclopédia de Vírus da Kaspersky Lab.

Os softwares potencialmente perigosos não têm uma função maliciosa, mas podem ser utilizados como componente auxiliar para um código malicioso, uma vez que contém falhas e erros. Esta categoria inclui, por exemplo, programas de administração remota, clientes de IRC, servidores de FTP, utilitários com várias finalidades para parar processos ou escondê-los, keyloggers (registadores de teclas digitadas), macros de password, autodialers (ligações telefónicas automáticas), etc. Tal software não é classificado como vírus, mas pode ser

dividido em diversos tipos, tais como Adware, Jokes, Riskware, etc. (para mais informação sobre programas potencialmente perigosos detectados pelo Kaspersky Anti-virus para Windows Workstations, veja a Enciclopédia de Vírus em www.viruslist.com). Como resultado da verificação, tais programas podem ser bloqueados. Visto que muitos deles são largamente utilizados pelos utilizadores, você tem a opção de os excluir da verificação. Para o fazer, tem que especificar o veredicto atribuído àquele programa como máscara de exclusão.

Por exemplo, no seu trabalho você usa, frequentemente, um programa de Administrador Remoto. Este é um sistema de acesso remoto com o qual você pode trabalhar a partir de um computador remoto. O Kaspersky Anti-virus para Windows Workstations este tipo de actividade de aplicação como sendo potencialmente perigosa e poderá bloqueá-la. Para evitar que a aplicação seja bloqueada, você tem que criar uma regra de exclusão que especifica como veredicto: *não é vírus:RemoteAdmin.Win32.RAdmin.22*.

Quando adiciona uma exclusão, é criada uma regra que as diversas componentes do programa (Anti-vírus de Ficheiros, Anti-vírus de E-mail, Anti-vírus de Internet, Defesa Pró-activa) e tarefas de verificação de vírus podem utilizar mais tarde. Você pode criar regras de exclusão numa janela especial que pode abrir a partir da janela de definições do programa, a partir da janela de aviso da detecção do objecto e a partir da janela de relatório.

Para adicionar exclusões ao Separador ***Regra de Exclusão****:*

1. Clicar no botão **Adicionar** no Separador **Máscara de Exclusão.**
2. Na janela que se abre (ver Figura 9), seleccione o tipo de exclusão na secção **Propriedades**:

☑ **Objecto** – exclui da verificação um determinado objecto, directório ou ficheiros que correspondem a uma determinada máscara.

☑ **Veredicto** – exclui um objecto da verificação, com base no seu estado a partir da classificação da Enciclopédia de Vírus.

Se você assinalar ambas as caixas ao mesmo tempo, será criada uma regra para aquele objecto com um determinado estado, de acordo com a classificação da Enciclopédia de Vírus. Nesse caso, aplicam-se as seguintes regras:

- Se especificar um determinado ficheiro como o **Objecto** e um determinado estado na secção **Veredicto**, o ficheiro especificado apenas será excluído se, durante a verificação, esse ficheiro for classificado como a ameaça seleccionada.
- Se seleccionar uma área ou pasta como o **Objecto** e o estado (ou máscara de veredicto) como o **Veredicto**, então os

objectos com aquele estado apenas serão excluídos da verificação naquela área ou pasta.

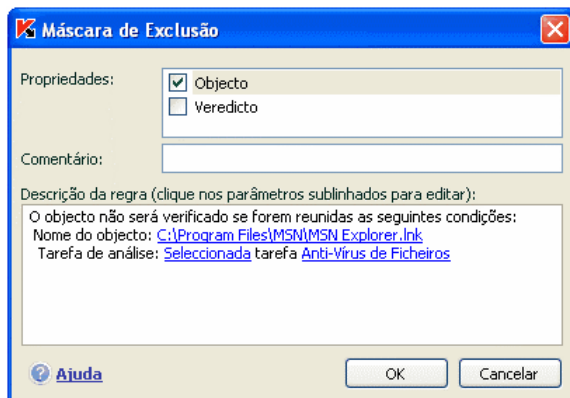



Figura 9. Criar uma máscara de exclusão

3. Especificar valores para os tipos de exclusão seleccionados. Para o fazer, na secção **Descrição da regra**, clique com o botão esquerdo do rato na ligação especificar localizada ao lado do tipo de exclusão:

- Para o tipo **Objecto**, insira o respectivo nome na janela que se abre (isto pode ser um ficheiro, uma pasta em particular ou uma máscara de ficheiro (ver A.2 na pág. 333). Assinale a opção **Incluir subpastas** para o objecto (ficheiro, máscara de ficheiro, pasta) ser recursivamente excluído da verificação. Por exemplo, se você especificou **C:\Program Files\winword.exe** como uma exclusão e assinalou a opção de verificação de pastas aninhadas, o ficheiro **winword.exe** será excluído da verificação se for encontrado nalguma pasta incluída em **C:\Program Files**.

- Insira o nome completo da ameaça que pretende excluir da verificação, tal como aparece definido na Enciclopédia de Vírus ou utilize uma máscara para o **Veredicto** (ver A.3 na pág. 333).

  Para algumas classificações, você pode especificar condições avançadas para a aplicação das regras no campo **Definições avançadas** (ver A.3 na pág. 333). Na maioria dos casos, este campo é, automaticamente, preenchido quando você adiciona uma regra de exclusão a partir de uma notificação da Defesa pró-activa.

Entre outros, pode adicionar definições avançadas para os seguintes veredictos:

- *Invasor*. Para este veredicto, você pode especificar um nome, máscara ou caminho completo para o objecto que se está a incorporar (por exemplo, um ficheiro .dll), enquanto uma condição adicional de exclusão.
- *Abrir Navegador da Internet.* Para este veredicto, você pode listar as definições de abertura do navegador de Internet, enquanto definições adicionais de exclusão. Por exemplo, você proibiu que os navegadores de Internet sejam abertos com determinadas definições no analisador da actividade das aplicações, na Defesa pró-activa. Contudo, enquanto regra de exclusão, você deseja permitir que o navegador de Internet seja aberto para o domínio www.kaspersky.com, através de um link a partir do Microsoft Office Outlook. Para o fazer, seleccione como **Objecto** de exclusão o Microsoft Office Outlook e como **Veredicto** *Abrir Navegador da Internet* e insira a máscara do domínio permitido no campo **Definições avançadas**.

4. Defina quais as componentes do Kaspersky Anti-virus para Windows Workstations que devem utilizar esta regra. Se seleccionar o item Em qualquer tarefa, esta regra será aplicada a todas as componentes. Se desejar restringir a regra a uma ou diversas componentes, clique na ligação Em qualquer, que se irá alterar para no/na tarefa. Na janela que se abre, assinale as caixas para as componentes às quais você pretende aplicar esta regra de exclusão.

Para criar uma regra de exclusão a partir da janela de notificação de que foi detectado um objecto perigoso:

1. Utilize a ligação Adicionar à zona confiável na janela de notificação (ver Figura 10).
2. Na janela que se abre, certifique-se de que todas as definições da regra de exclusão estão de acordo com o que pretende. O nome do objecto e tipo de ameaça, atribuídos ao objecto, estão automaticamente preenchidos, com base na informação do notificação. Para criar a regra, clique em **OK**.

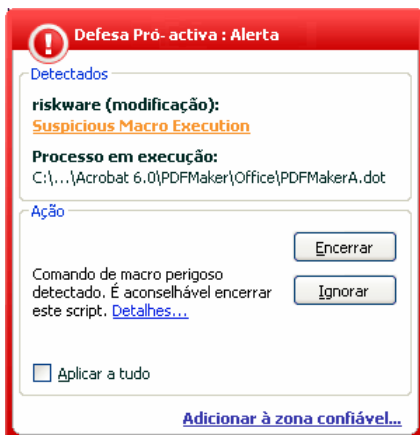



Figura 10. Notificação de detecção de objecto perigoso

Para criar uma regra de exclusão a partir da janela de relatório:

1. No relatório, seleccione o objecto que pretende adicionar às exclusões.
2. Abra o menu de contexto e seleccione **Adicionar à Zona Confiável** (ver Figura 11).
3. Como resultado, abrir-se-á a janela de definições da exclusão. Certifique-se de que todas as definições da regra de exclusão estão de acordo com o que pretende. O nome do objecto e tipo de ameaça, atribuídos ao objecto, estão automaticamente preenchidos, com base na informação do relatório. Para criar a regra, clique em **OK**.

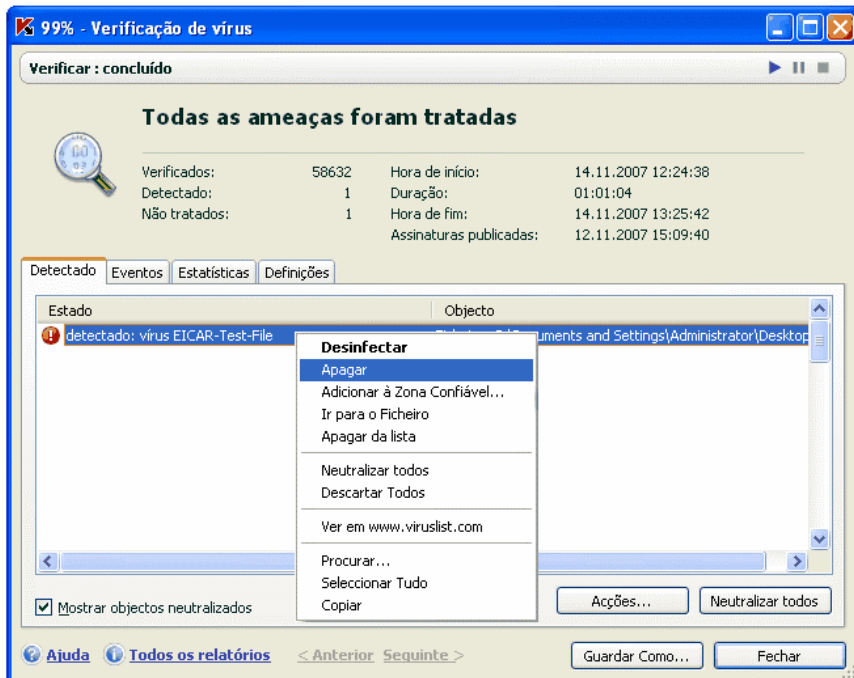



Figura 11. Criar uma regra de exclusão a partir de um relatório

6.3.2. Aplicações confiáveis

Apenas pode excluir da verificação aplicações confiáveis no Kaspersky Anti-virus, se este estiver instalado num computador com o Microsoft Windows NT 4.0/2000/XP/Vista.

O Kaspersky Anti-virus permite criar uma lista de aplicações confiáveis, cuja actividade, ficheiros, rede e acesso ao registo do sistema não são monitorizados, seja essa actividade suspeita ou de outro tipo.

Por exemplo, você acha que os objectos utilizados pelo Windows **Notepad** são seguros e não necessitam de ser verificados. Ou seja, você confia nos processos deste programa. Para excluir da verificação os objectos utilizados por este processo, adicione o **Notepad** à lista de aplicações confiáveis. Contudo, o ficheiro executável e o processo da aplicação confiável serão verificados, quanto à existência de vírus, tal como antes. Para excluir completamente essa aplicação (da tarefa de verificação), você deve usar as regras de exclusão (ver 6.3.1 na pág. 78).

Para além disso, algumas acções classificadas como perigosas são perfeitamente normais para as funcionalidades de alguns programas. Por exemplo, programas que alternam automaticamente a disposição do teclado, tais como o Punto Switcher, normalmente interceptam o texto inserido no seu teclado. Para incorporar esses programas e deixar de monitorizar a sua actividade, recomendamos que os adicione à lista de aplicações confiáveis.

A utilização das exclusões de aplicações confiáveis também pode resolver potenciais conflitos de compatibilidade entre o Kaspersky Anti-virus para Windows Workstations e outras aplicações (por exemplo, o tráfego de rede de outro computador que já foi analisado pela aplicação de anti-vírus) e pode incrementar a produtividade do computador, o que é especialmente importante quando se utilizam aplicações de servidor.

Por defeito, o Kaspersky Anti-virus para Windows Workstations verifica objectos abertos, executados ou guardados por qualquer processo de programa e monitoriza a actividade de todos os programas e o tráfego de rede que eles geram.

Pode criar uma lista de aplicações confiáveis no Separador especial **Aplicações Confiáveis** (ver Figura 12). Por defeito, a lista de aplicações confiáveis contém uma lista das aplicações que não serão monitorizadas, com base nas recomendações da Kaspersky Lab quando instala o Kaspersky Anti-virus. Se não confia numa aplicação existente na lista, desmarque a caixa correspondente. Pode editar a lista utilizando os botões do lado direito **Adicionar**, **Editar** e **Apagar**.

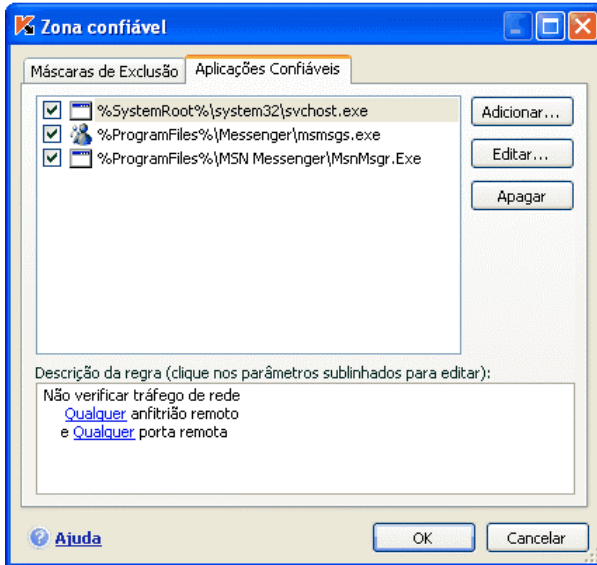



Figura 12. Lista de aplicações confiáveis

Para adicionar um programa à lista de aplicações confiáveis:

1. Clique no botão **Adicionar** no lado direito do separador **Aplicações Confiáveis**.
2. Na janela **Aplicação Confiável** (ver Figura 13) que se abre, seleccione a aplicação utilizando o botão **Procurar**. Abrir-se-á um menu de contexto e, ao clicar em **Procurar**, pode ir para a janela de selecção de ficheiro e seleccionar o atalho para o ficheiro executável ou, clicando **Aplicações,** pode ir para uma lista das aplicações actualmente em funcionamento e seleccionar as necessárias.

Quando selecciona um programa, o Kaspersky Anti-virus para Windows Workstations retém os atributos internos do ficheiro executável e usa-os para identificar o programa como confiável durante as verificações.

O caminho do ficheiro é introduzido automaticamente quando selecciona o respectivo nome.

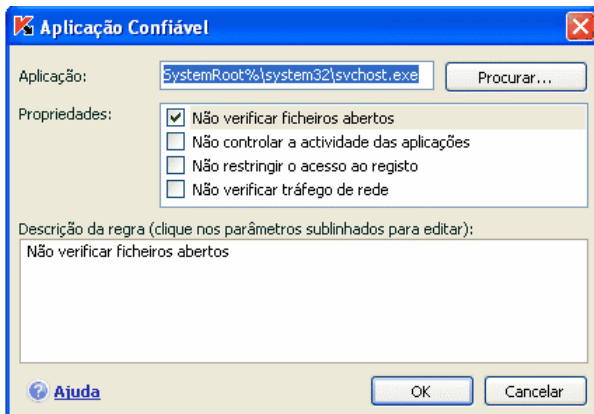



Figura 13. Adicionar uma aplicação à lista de aplicações confiáveis

3. Depois especifique quais as acções executadas por este processo que não serão monitorizadas:

   ☑ **Não verificar ficheiros abertos** – exclui da verificação todos os ficheiros que o processo da aplicação confiável abrir.

   ☑ **Não controlar a actividade das aplicações** – exclui da Defesa Pró-activa qualquer actividade, suspeita ou de outro tipo, que a aplicação confiável estiver a executar.

   ☑ **Não restringir o acesso ao registo** – exclui da verificação as tentativas de acesso ao registo do sistema, quando iniciadas pelas aplicações confiáveis.

   ☑ **Não verificar tráfego de rede** – exclui, da verificação de vírus e spam, o tráfego de rede que a aplicação confiável iniciar. Você pode excluir da verificação todo o tráfego de rede da aplicação ou tráfego encriptado (SSL). Para o fazer, clique na ligação Em qualquer, que mudará para encriptado. Para além disso, pode restringir a exclusão, especificando um determinado anfitrião remoto ou porta remota. Para criar uma restrição, clique na ligação Em qualquer, que mudará para no/na e insira um valor para a porta remota/anfitrião remoto.

> Note que se a opção ☑ **Não verificar tráfego de rede** estiver assinalada, o tráfego para aquela aplicação apenas será verificado quanto à presença de vírus e spam. Contudo, isto não afecta o facto de o Anti-Hacker verificar ou não o tráfego. As definições do Anti-Hacker administram a análise da actividade de rede para aquela aplicação.

6.4. Iniciar tarefas com outro perfil

O Kaspersky Anti-virus para Windows Workstations possui uma funcionalidade que pode iniciar a tarefas de verificação e actualizações com outro perfil de utilizador. Por defeito, esta funcionalidade está desactivada e as tarefas são executadas de acordo com o perfil com a qual você está registado no sistema.

Por exemplo, você poderá precisar de direitos de acesso a um certo ficheiro durante uma verificação. Ao utilizar esta funcionalidade, pode configurar tarefas para funcionarem segundo outro perfil de utilizador que possua os privilégios necessários.

Note que esta opção não está disponível com o Microsoft Windows 98/ME.

As actualizações do programa podem ser feitas a partir de uma origem à qual você não pode aceder (por exemplo, a pasta de actualização de rede ou direitos de utilizador autorizados para um servidor proxy). Pode utilizar esta funcionalidade para pôr o Actualizador a funcionar com outro perfil que possua esse direitos.

Para configurar uma tarefa de verificação com outro perfil de utilizador:

1. Seleccione o nome da tarefa na secção **Verificar** (para verificações de vírus) ou a secção **Serviço** (para tarefas de actualização) da janela principal e use a ligação Definições para abrir a janela de definições da tarefa.

2. Clique no botão **Personalizar** na janela de definições da tarefa e aceda ao separador **Adicional** na janela que se abre (ver Figura 14).

Para activar esta funcionalidade, seleccione ☑ **Executar esta tarefa como...** Introduza os dados de acesso com os quais você quer iniciar a tarefa: nome de utilizador (conta) e password.

Note que se não executar a tarefa com privilégios, a actualização agendada será executada com os privilégios da actual conta de utilizador. Se não estiverem registados utilizadores no computador, se a execução de actualizações com outra conta de utilizador não estiver configurada e se as actualizações foram executadas de forma automática, estas serão executadas com privilégios de SISTEMA.

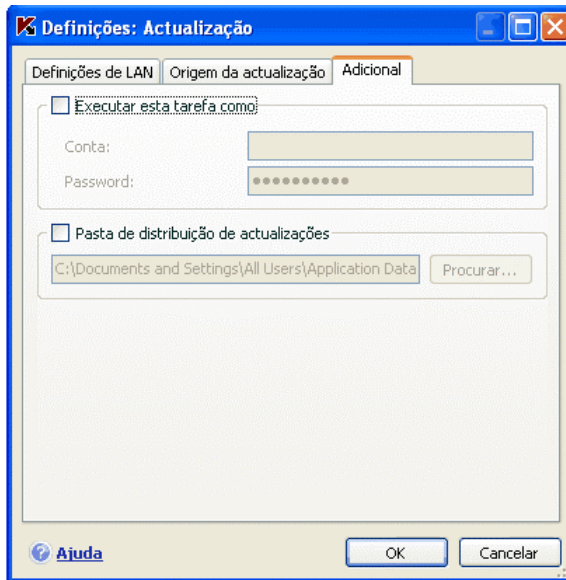



Figura 14. Configurar tarefa de actualização com outro perfil

6.5. Configurar Tarefas e Notificações Agendadas

A configuração de um agendamento é idêntica para as tarefas de verificação de vírus, as actualizações da aplicação e para as notificações de eventos do Kaspersky Anti-Virus.

Por defeito, a definição de agendamento está desligada para as tarefas criadas quando a aplicação é instalada. A única excepção é a verificação dos objectos de inicialização, que é executada sempre que inicia o Kaspersky Anti-Virus. Por defeito, as actualizações estão configuradas para ocorrerem, automaticamente, à medida que ficarem disponíveis nos servidores de actualização da Kaspersky Lab.

Caso não esteja satisfeito com estas definições, pode reconfigurar o agendamento. Seleccione uma tarefa pelo seu nome por baixo de **Verificar** (para tarefas de verificação de vírus) ou a secção **Serviço** (para actualizações e distribuição de actualizações) e abra a respectiva janela de definições, clicando em Definições.

Para que as tarefas sejam iniciadas de acordo com um horário agendado, assinale a caixa de início automático da tarefa na secção **Modo de Execução**. Pode editar as condições para iniciar a tarefa de verificação na janela **Agendamento** (ver Figura 15), que se abre quando clica em **Alterar**.

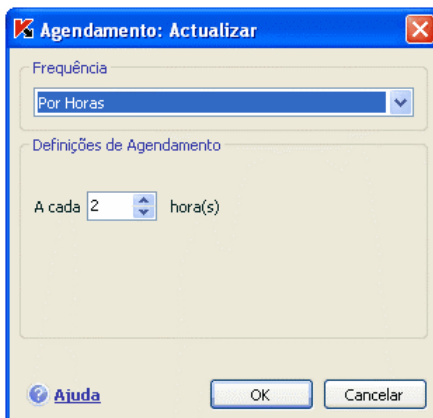



Figura 15. Configurar agendamento de tarefas

O primeiro valor a definir é a frequência de um evento (execução da tarefa ou notificação). Seleccione a opção desejada na secção **Frequência** (ver Figura 15). Depois, as definições para a opção seleccionada devem ser especificadas em Definições de Agendamento. Pode seleccionar uma das seguintes opções:

- **Minutos.** O intervalo de tempo entre execuções da tarefa ou notificações será de vários minutos. Defina o intervalo de tempo em minutos nas definições de agendamento. Não deverá exceder os 59 minutos.
- **Horas.** O intervalo entre execuções da tarefa ou notificações será de várias horas. Se escolher esta opção, especifique o intervalo de tempo nas definições de agendamento: **A cada n hora(s)** e defina *N*. Por exemplo, especifique **A cada 1 hora(s)** para executar de hora em hora.
- **Dias.** As tarefas serão iniciadas ou as notificações serão em enviadas com um intervalo de alguns dias. Especifique a duração do intervalo nas definições de agendamento:
  - Seleccione **A cada N dias** e especifique o valor para *N* se deseja ter um intervalo de um determinado número de dias..
  - Seleccione **Todos os dias da semana**, se pretende executar as tarefas diariamente, de Segunda a Sexta-feira.
  - Seleccione **Todos os fins-de-semana** para as tarefas serem executadas apenas aos Sábados e Domingos.

Use o campo **Hora** para especificar a que hora do dia a tarefa será executada.

- **Semanas**. As tarefas serão iniciadas ou as notificações serão enviadas em certos dias da semana. Se seleccionar esta opção de frequência, assinale com um visto os dias da semana nos quais as tarefas serão executadas com as definições de agendamento. Use o campo **Hora** para definir a hora.
- **Mensalmente**. As tarefas serão iniciadas ou as notificações serão enviadas uma vez por mês à hora especificada.
- **A uma hora especificada.** Inicia a tarefa ou envia a notificação no dia e à hora que especificar.
- **Com a inicialização da aplicação**. Executa a tarefa ou envia a notificação sempre que inicia o Kaspersky Anti-Virus. Também pode especificar um tempo de espera para executar a tarefa depois de iniciar a aplicação.
- **Após cada actualização**. A tarefa é executada após cada actualização das bases de dados da aplicação (esta opção apenas se aplica às tarefas de verificação de vírus).

Se, por alguma razão, uma tarefa não puder ser executada (por exemplo, não estava instalado um programa de e-mail ou computador não estava ligado àquela hora), pode configurar a tarefa para ser automaticamente executada assim que for possível. Assinale a opção **Executar tarefa se tiver sido ignorada** na janela de agendamento.

6.6. Opções de energia

Para conservar a bateria do seu computador portátil e para reduzir a carga no processador central e subsistemas do disco, você pode adiar as verificações de vírus:

- Uma vez que, por vezes, que as verificações de vírus e as actualizações do programa exigem uma quantidade razoável de recursos e podem demorar algum tempo, recomendamos que desactive os agendamentos destas tarefas. Isto ajudá-lo-á a poupar o tempo de vida da bateria. Se necessário, você mesmo poderá actualizar o programa (ver 5.6 na pág. 69) ou iniciar uma verificação de vírus. Para utilizar a funcionalidade de poupança de energia, seleccione a caixa **Desactivar verificações agendadas quando o computador estiver a funcionar com bateria**.
- As verificações de vírus aumentam a carga no processador central e nos subsistemas do disco, diminuindo assim a actividade de outros programas. Por definição, se esta situação acontecer, o programa

suspenderá as verificações de vírus e libertará recursos do sistema para as aplicações do utilizador.

No entanto, existem certos programas que podem ser lançados assim que os recursos do processador são libertados e funcionam em segundo plano. Para que as análises de vírus não dependam do funcionamento de tais programas, desmarque a opção ☑ **Conceder recursos para outras aplicações**.

Note que esta definição pode ser configurada, individualmente, para cada tarefa de verificação de vírus. Se escolher fazê-lo, a configuração para uma tarefa específica tem uma prioridade mais elevada.

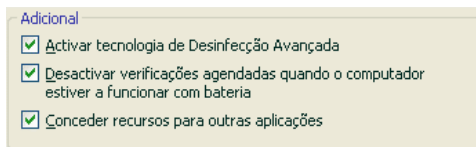



Figura 16. Configurar Opções de energia

Para configurar opções de energia para tarefas de verificação de vírus:

Seleccione a secção **Protecção** da janela principal do programa e clique na ligação Definições. Configure as opções de energia na caixa **Adicional** (ver Figura 16).

6.7. Tecnologia de Desinfecção Avançada

Actualmente, os programas maliciosos conseguem invadir os níveis mais baixos de um sistema operativo, o que os torna, praticamente, impossíveis de apagar. O Kaspersky Anti-virus 6.0 pergunta-lhe se deseja executar a Tecnologia de Desinfecção Avançada quando este detectar uma ameaça actualmente activa no sistema. Isto irá neutralizar a ameaça e apagá-la do computador.

Após este procedimento, você precisará de reiniciar o seu computador. Depois de reiniciar o computador, recomendamos que execute uma verificação completa de vírus. Para usar a Tecnologia de Desinfecção Avançada, assinale a opção ☑ **Activar tecnologia de Desinfecção Avançada**.

Para activar/desactivar a tecnologia de desinfecção avançada:

Seleccione a secção **Protecção** da janela principal do programa e clique na ligação Definições. Configure as opções de energia na secção **Adicional** (ver Figura 16).

CAPÍTULO 7. ANTI-VÍRUS DE FICHEIROS

No Kaspersky Anti-virus para Windows Workstations está incluída uma componente especial para proteger os ficheiros do seu computador em relação a uma infecção, o *Anti-vírus de Ficheiros.* Esta componente é iniciada quando inicia o seu sistema operativo e é executada na Memória de Acesso Aleatório (RAM) do seu computador e verifica todos os ficheiros que abre, guarda ou executa.

O indicador do funcionamento da componente é apresentado no ícone de bandeja do sistema do Kaspersky Anti-virus para Windows Workstations, que apresenta este aspecto sempre que um ficheiro está a ser verificado.

Por defeito, o Anti-vírus de Ficheiros apenas verifica ficheiros *novos ou modificados*, ou seja, ficheiros que foram adicionados ou modificados desde a verificação anterior. Os ficheiros são verificados de acordo com o seguinte algoritmo:

1. Cada ficheiro que o utilizador ou um programa utiliza é interceptado pela componente.
2. O Anti-vírus de Ficheiros verifica as bases de dados das tecnologias iChecker™ e iSwift™, procurando informação sobre o ficheiro interceptado. Com base na informação recolhida, é tomada uma decisão sobre se verificar ou não o ficheiro.

O processo de verificação inclui os seguintes passos:

1. O ficheiro é analisado em termos da presença de vírus. Os objectos maliciosos são detectados por comparação com as *assinaturas de ameaças* utilizadas pelo programa. As assinaturas contêm descrições de todos os programas maliciosos, ameaças e ataques de rede conhecidos até à data e dos métodos para os neutralizar.
2. Depois da análise, estão disponíveis as seguintes opções de comportamento:
   a. Se for detectado um código malicioso no ficheiro, o Anti-vírus de Ficheiros bloqueia o ficheiro, coloca uma cópia do mesmo na *cópia de segurança* e tenta neutralizar o ficheiro. Se o ficheiro for desinfectado com sucesso, o mesmo passa a estar novamente disponível. Se a desinfecção não for possível, o ficheiro é apagado.

b. Se num ficheiro for detectado um código que parece ser malicioso, mas não existir uma certeza absoluta, o ficheiro é sujeito a desinfecção e enviado para a *Quarentena*.

c. Se não for descoberto nenhum código malicioso no ficheiro, o mesmo é imediatamente restaurado.

7.1. Seleccionar um nível de segurança dos ficheiros

O Anti-vírus de Ficheiros protege os ficheiros que está a utilizar com um dos seguintes níveis (ver Figura 17):

Elevado – o nível com a monitorização mais abrangente dos ficheiros que abre, guarda ou executa.

Recomendado – Os especialistas da Kaspersky Lab recomendam este nível de segurança. Permite verificar as seguintes categorias de objectos:

- Programas e documentos por conteúdo
- Objectos novos ou modificados desde a última verificação
- Objectos OLE incorporados

Baixo – Nível com definições que lhe permitem utilizar, de forma confortável, as aplicações que requerem mais recursos do sistema, uma vez que o conjunto de ficheiros a ser verificado é menor.

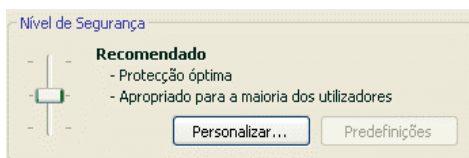



Figura 17. Nível de Segurança do Anti-vírus de Ficheiros

Por defeito, o Anti-vírus de Ficheiros está definido no nível **Recomendado**.

Pode aumentar ou baixar o nível de protecção, seleccionando o nível que pretende ou alterando as definições do nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio de velocidade de verificação e o total de ficheiros verificados: quanto menos ficheiros forem sujeitos a verificação em termos de vírus, maior é a velocidade de verificação.

Se nenhum dos níveis de segurança definidos responder às suas necessidades, você pode personalizar as definições de protecção. Para o fazer, seleccione o nível que está mais próximo daquilo que necessita, como ponto de partida, e edite as suas definições. Nesse caso, o nível será estabelecido como **Definições Personalizadas**. Vamos examinar um exemplo de como pode ser útil ter um nível de segurança de ficheiros definido pelo utilizador.

Exemplo:

O trabalho que desenvolve no seu computador implica o uso de um número elevado de tipos de ficheiros diferentes, alguns dos quais podem ser consideravelmente grandes. Você não quer correr o risco de ignorar ficheiros na verificação devido ao seu tamanho ou extensão, mesmo que isto possa afectar a produtividade do seu computador.

Dica para seleccionar um nível de segurança:

Tendo em conta os dados disponíveis, pode-se concluir que existe um risco consideravelmente elevado de se ter uma infecção por um programa malicioso. O tamanho e o tipo de ficheiros a serem tratados é bastante variado e ignorá-los na verificação poderia colocar em risco a informação do seu computador. O requisito básico para a verificação é analisar os ficheiros tratados de acordo com os seus conteúdos, em vez de pela sua extensão.

Recomenda-se que utilize o nível **Recomendado** como o seu nível de segurança básico pré-instalado, inserindo depois as seguintes alterações: remova a restrição sobre o tamanho dos ficheiros a serem verificados e optimize o funcionamento do Anti-vírus de Ficheiros, limitando a verificação aos ficheiros novos e modificados. Neste caso, será diminuída a carga sobre o computador ao verificar os ficheiros, de forma a que possa utilizar, de forma confortável, as outras aplicações.

Para modificar as definições para um nível de segurança:

Clique no botão **Personalizar** na janela de definições do Anti-vírus de Ficheiros. Edite as definições do Anti-vírus de Ficheiros na janela que se abre e clique **OK**.

Desta maneira, será criado um quarto nível de segurança, **Definições Personalizadas**, que contém as definições de protecção que você configurou.

7.2. Configurar o Anti-vírus de Ficheiros

A configuração determina a forma como o Anti-vírus de Ficheiros será executado no seu computador. As definições podem ser desagregadas nos seguintes grupos:

- Definições que definem que tipos de objectos que serão verificados (ver 7.2.1 na pág. 95) quanto à existência de vírus
- Definições que definem o âmbito de protecção (ver 7.2.2 na pág. 98)
- Definições que definem a forma como é que o programa responde aos objectos perigosos (ver 7.2.5 na pág. 102)
- Definições adicionais do Anti-vírus de Ficheiros (ver 7.2.3 na pág. 100)

As secções que se seguem irão examinar, em detalhe, os grupos acima listados.

7.2.1. Definir os tipos de ficheiros a serem verificados

Ao especificar os tipos de ficheiros que serão verificados, você estabelece que formatos de ficheiros, que tamanhos e que unidades serão verificadas, em termos de vírus, quando abertos, executados ou guardados.

Para facilitar a configuração, os ficheiros são divididos em dois grupos: *simples e compostos*. Os ficheiros simples não contêm quaisquer objectos. Os ficheiros compostos podem incluir vários objectos, cada um dos quais poderão vários níveis de encadeamento. Existem muitos exemplos: arquivos, ficheiros que contêm macros, tabelas, e-mails com anexos, etc.

Os tipos de ficheiros analisados são definidos na secção **Tipos de ficheiros** (ver Figura 18). Seleccione uma das três opções que se seguem:

Verificar todos os ficheiros. Com esta opção seleccionada, todos os objectos do sistema que estiverem abertos, a funcionar, ou guardados serão analisados sem excepção.

Programas e documentos (por conteúdo). Se seleccionar este grupo de ficheiros, o Anti-vírus de Ficheiros só analisará ficheiros potencialmente infectados – ficheiros nos quais um vírus se poderia inserir.

Nota:

Existem alguns formatos de ficheiros que têm um risco relativamente reduzido de possuírem código malicioso inserido neles e, subsequentemente, ser activado. Um exemplo são os ficheiros txt. Por outro lado, existem formatos de ficheiros que contém ou podem conter código executável. Os exemplos são os formatos .exe, .dll, ou .doc. Nesses ficheiros, o risco de inserção e activação de código malicioso é relativamente elevado.

Antes de procurar vírus num ficheiro, é analisado o seu cabeçalho interno no que concerne ao formato de ficheiro (txt, doc, exe, etc.). Se os resultados da verificação demonstrarem que o formato do ficheiro é do tipo dos que não podem ser infectados, esse ficheiro não é verificado em termos de vírus e é imediatamente restaurado para uso. Se o formato de ficheiro permite que o ficheiro seja infectado, esse ficheiro é verificado quanto à existência de vírus.

Programas e documentos (por extensão). Se seleccionar esta opção, o Anti-vírus de Ficheiros só analisará ficheiros potencialmente infectados, mas o formato do ficheiro será determinado pela extensão. Utilizando a ligação extensão, pode examinar uma lista das extensões de ficheiros que são verificados neste caso (ver A.1 na pág. 329).

Dica:

Não se esqueça que alguém pode enviar um vírus para o seu computador com uma extensão (.txt por exemplo) que é na realidade um ficheiro executável renomeado como um ficheiro .txt. Se seleccionar a opção **Programas e documentos (por extensão)**, a verificação ignoraria tal ficheiro. Se a opção **Programas e documentos (por conteúdo)** for seleccionada, a extensão é ignorada e a análise dos cabeçalhos dos ficheiros revelará que o ficheiro é um ficheiro .exe. O Anti-vírus de Ficheiros verificaria o ficheiro, em profundidade, quanto à existência de vírus.

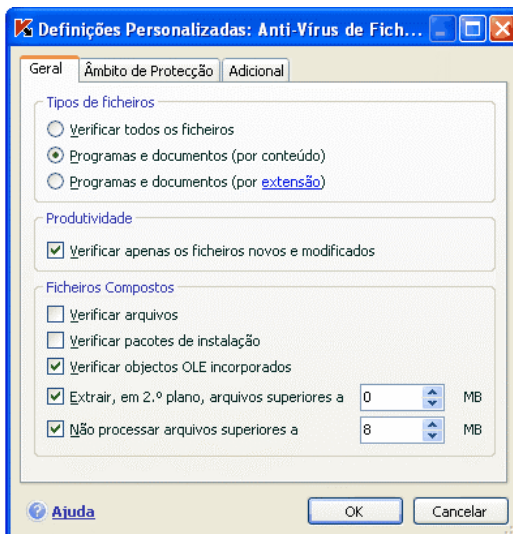



Figura 18. Seleccionar os tipos de ficheiros analisados

Na secção **Produtividade**, poderá especificar que apenas deverão ser analisados, quanto à presença de vírus, os ficheiros novos ou os ficheiros que foram modificados desde a última verificação. Este modo de funcionamento reduz, significativamente, o tempo de verificação e aumenta a velocidade de desempenho do programa. Para o fazer, deve escolher a opção ☑ **Verificar apenas os ficheiros novos e modificados**. Este modo estende-se aos ficheiros simples e compostos.

Na secção **Ficheiros Compostos**, especifique que ficheiros compostos devem ser analisados:

☑ **Verificar Arquivos** – verifica arquivos .zip, .cab, .rar e .arj.

☑ **Verificar pacotes de instalação** – analisa arquivos de extracção automática.

☑ **Verificar objectos OLE incorporados** – verifica objectos incorporados em ficheiros (por exemplo, folhas de cálculo do Microsoft Office Excel ou uma macro inserida num ficheiro do Microsoft Office Word, anexos de e-mail, etc.).

Para cada tipo de ficheiro composto, você pode seleccionar e verificar todos os ficheiros ou apenas os ficheiros novos. Para o fazer, utilize a ligação que surge antes do nome do objecto. Esta ligação altera-se quando clica com o botão esquerdo do rato sobre a mesma. Se a secção **Optimização** foi definida para apenas verificar ficheiros novos e modificados, você não conseguirá seleccionar o tipo de ficheiros compostos a serem verificados.

Para especificar quais os ficheiros compostos que não deverão ser verificados quanto a vírus, utilize as seguintes definições:

☑ **Extrair, em 2.º plano, arquivos superiores a... MB.** Se o tamanho de um ficheiro composto exceder esta restrição, o programa irá verificá-lo enquanto um objecto único (analisando o cabeçalho) e irá devolvê-lo ao utilizador. Os objectos que esse ficheiro contém serão verificados mais tarde. Se esta caixa não estiver assinalada, o acesso a ficheiros superiores ao tamanho indicado será bloqueado até que os mesmos sejam verificados.

☑ **Não processar arquivos superiores a... MB.** Neste caso, os ficheiros superiores ao tamanho especificado serão ignorados pela verificação.

7.2.2. Definir o âmbito de protecção

Por defeito, o Anti-vírus de Ficheiros verifica todos os ficheiros quando estes são utilizados, independentemente de onde estiverem armazenados, seja num disco rígido, num CD/DVD-ROM ou num disco flash.

Você pode limitar o âmbito de protecção. Para o fazer:

1. Seleccione o **Anti-vírus de Ficheiros** na janela principal e aceda à janela de definições de componente clicando em Definições.

2. Clique no botão **Personalizar** e seleccione o Separador **Âmbito de Protecção** (ver Figura 19) na janela que se abre.

O separador apresenta uma lista dos objectos que o Anti-vírus de Ficheiros irá verificar. Por defeito, a protecção está activada para todos os objectos existentes em discos rígidos, meios removíveis e unidades de rede ligadas ao seu computador. Você pode adicionar objectos à lista ou editar a lista, utilizando os botões **Adicionar**, **Editar** e **Apagar**.

Se pretender limitar o conjunto de objectos protegidos, pode fazê-lo utilizando os seguintes métodos:

- Especificar apenas as pastas, unidades e ficheiros que precisam de ser protegidos.
- Criar uma lista de objectos que não necessitam ser protegidos (ver 6.3 na pág. 77).
- Combinar os métodos um e dois – criar um âmbito de protecção a partir do qual alguns objectos são excluídos.

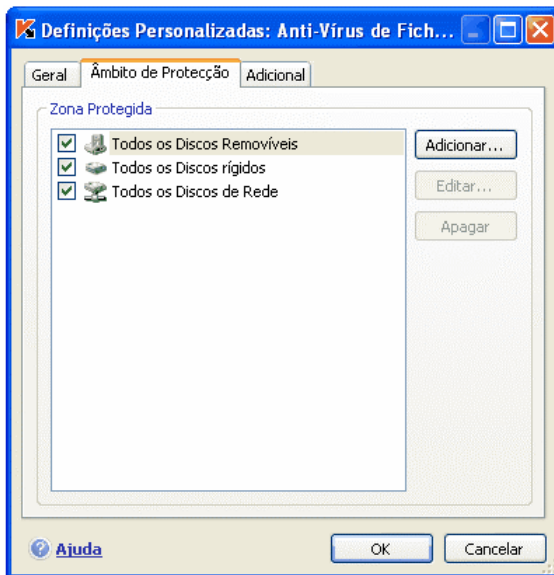



Figura 19. Definir o âmbito de protecção

Pode usar máscaras quando adiciona objectos para verificação. Note que apenas pode inserir máscaras com caminhos absolutos para os objectos:

- **C:\dir*.*** ou **C:\dir*** ou **C:\dir** - todos os ficheiros na pasta *C:\dir*
- **C:\dir*.exe** - todos os ficheiros com a extensão *.exe* na pasta *C:\dir*
- **C:\dir*.ex?** – todos os ficheiros com a extensão *.ex?* na pasta *C:\dir*, onde ? pode representar qualquer caractere único
- **C:\dir\teste** – apenas o ficheiro *C:\dir\teste*

Para que a verificação seja executada de forma recursiva, marque a opção ☑ **Incluir subpastas**.

> Atenção!
>
> Lembre-se que o Anti-vírus de Ficheiros irá verificar apenas os ficheiros que estão incluídos no âmbito de protecção que foi criado. Os ficheiros que não estão incluídos nesse âmbito estarão disponíveis para serem utilizados sem verificação. Isto aumenta o risco de uma infecção no seu computador.

7.2.3. Configurar definições avançadas

Nas definições adicionais do Anti-vírus de Ficheiros pode especificar o modo de verificação do sistema de ficheiros e configurar as condições para pausar, temporariamente, a componente.

Para configurar definições adicionais do Anti-vírus de Ficheiros:

1. Seleccione o **Anti-vírus de Ficheiros** na janela principal e acede à janela de definições da componente, clicando na ligação Definições.

2. Clique no botão **Personalizar** e seleccione o separador **Adicional** na janela que se abre (ver Figura 20).

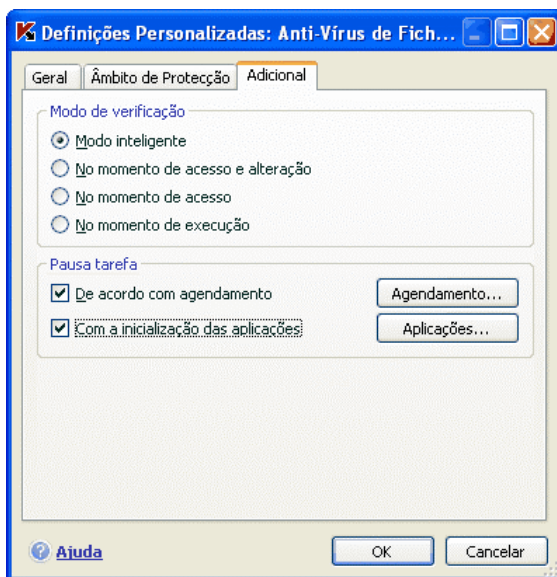



Figura 20. Configurar definições adicionais do Anti-vírus de Ficheiros

O modo de verificação determina as condições de processamento do Anti-vírus de Ficheiros. Dispõe das seguintes opções:

- **Modo inteligente**. Este modo destina-se a acelerar o processamento de ficheiros e a devolvê-los ao utilizador. Quando é seleccionado, a decisão de verificar é tomada com base na análise das operações efectuadas com o ficheiro.

  Por exemplo, quando utilizar um ficheiro do Microsoft Office, o Kaspersky Anti-virus verifica o ficheiro, primeiro, quando este é aberto e, por último,

quando este é fechado. Todas as operações intermédias gravadas no ficheiro não são verificadas.

O modo inteligente é a opção predefinida.

- **No momento de acesso e alteração** – O Anti-vírus de Ficheiros verifica os ficheiros assim que são abertos ou editados.
- **No momento de acesso** – apenas verifica os ficheiros quando é feita uma tentativa para os abrir.
- **No momento de execução** – apenas verifica dos ficheiros quando é feita uma tentativa para os executar.

Pode precisar de pausar o Anti-vírus de Ficheiros ao executar tarefas que requerem recursos significativos do sistema operativo. Para reduzir a carga sobre o processador e garantir que o utilizador recupera, rapidamente, o acesso aos ficheiros, recomendamos que configure a componente para se desactivar a uma determinada hora ou enquanto determinados programas estiverem a ser utilizados.

Para pausar a componente durante um determinado período de tempo, assinale a opção ☑ **De acordo com agendamento** e, na janela que se abre (ver Figura 21) clique em **Agendamento** para atribuir um período de tempo para desactivar e retomar a componente. Para o fazer, introduza um valor no formato HH:MM nos campos correspondentes.

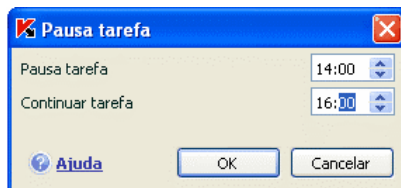



Figura 21. Pausar a componente

Para desactivar a componente quando trabalhar com programas que requeiram recursos significativos, assinale a opção ☑ **Com a inicialização das aplicações** e edite a lista de programas na janela que se abre (ver Figura 22), clicando em **Aplicações**.

Para adicionar uma aplicação à lista, utilize o botão **Adicionar**. Abrir-se-á um menu de contexto e, se clicar em **Procurar**, você pode ir para a janela padrão de selecção de ficheiro e especificar o ficheiro executável da aplicação a adicionar. Em alternativa, aceda à lista de aplicações, actualmente, em execução, a partir do item **Aplicações** e seleccione a que desejar.

Para apagar uma aplicação, seleccione-a da lista e clique em **Apagar.**

Pode desactivar, temporariamente, a pausa a efectuar no Anti-vírus ao utilizar uma aplicação específica. Para o fazer, desmarque o nome da aplicação. Não tem que a apagar da lista.

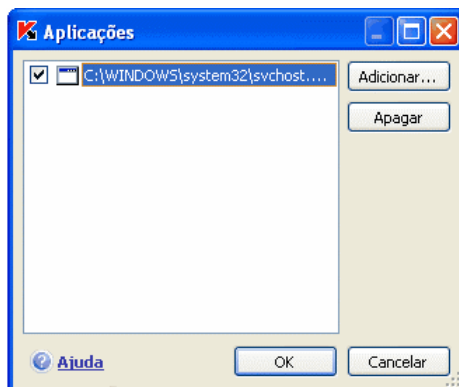



Figura 22. Criar uma lista de aplicações

7.2.4. Restaurar as predefinições do Anti-vírus de Ficheiros

Ao configurar o Anti-vírus de Ficheiros, pode sempre voltar às opções de desempenho recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as no nível de segurança **Recomendado**.

Para restaurar as predefinições do Anti-vírus de Ficheiros:

1. Seleccione o **Anti-vírus de Ficheiros** na janela principal e aceda à janela de definições da componente, clicando em Definições.

2. Clique no botão **Predefinições** na secção **Nível de Segurança**.

Ao configurar as definições do Anti-vírus de Ficheiros, se tiver alterado a lista de objectos incluídos na zona protegida, o programa perguntar-lhe-á se deseja guardar aquela lista para uso futuro, quando restaurar as definições iniciais. Para guardar a lista de objectos, assinale a opção **Âmbito de Protecção** na janela que se abre: **Restaurar definições**.

7.2.5. Seleccionar acções para objectos

Quando, ao verificar um ficheiro quanto à existência de vírus, se descobrir que o mesmo está infectado ou se suspeitar que está infectado, as acções

subsequentes do Anti-vírus de Ficheiros dependem do estado dos objectos e da acção seleccionada.

O Anti-vírus de Ficheiros pode classificar um objecto com um dos seguintes estados:

- Estado de programa malicioso (por exemplo, vírus, Trojan).
- *Potencialmente infectado,* quando a verificação não consegue determinar se o objecto está infectado. Isto significa que o código do ficheiro contém uma secção de código que se assemelha a um vírus conhecido mas alterado ou que faz lembrar a estrutura de uma sequência de vírus.

Por defeito, todos os ficheiros infectados são sujeitos a desinfecção e se estiverem potencialmente infectados, então são enviados para a Quarentena.

Para alterar uma acção para um objecto:

Seleccione o **Anti-vírus de Ficheiros** na janela principal e aceda à janela de definições da componente, clicando em Definições. Todas as acções possíveis são apresentadas nas secções apropriadas (ver Figura 23).

Figura 23. Acções possíveis do Anti-vírus de Ficheiros em relação a objectos perigosos

Se a acção seleccionada foi:	Quando é detectado um objecto perigoso:
Perguntar o que fazer	O Anti-vírus de Ficheiros exibe uma mensagem de aviso que contém informação sobre qual o programa malicioso que infectou ou infectou potencialmente o ficheiro e dá-lhe à escolha uma das seguintes acções. Dependendo do estado do objecto, as acções podem variar.

Se a acção seleccionada foi:	Quando é detectado um objecto perigoso:
Bloquear acesso	O Anti-vírus de Ficheiros bloqueia o acesso ao objecto. A informação acerca disto é gravada no relatório (ver 17.3 na pág. 245). Poderá tentar desinfectar este objecto mais tarde.
Bloquear acesso ☑ **Desinfectar**	O Anti-vírus de Ficheiros vai bloquear o acesso ao objecto e tentar desinfectá-lo. Se for desinfectado com sucesso, esse objecto é restaurado para utilização regular. Se a desinfecção falhar, será atribuído o estado de *potencialmente infectado* ao ficheiro e este será movido para a Quarentena (ver 17.1 na pág. 239). A informação acerca disto é gravada no relatório. Mais tarde, você pode tentar desinfectar este objecto.
Bloquear acesso ☑ **Desinfectar** ☑ **Apagar se a desinfecção falhar**	O Anti-vírus de Ficheiros vai bloquear o acesso ao objecto e vai tentar desinfectá-lo. Se for desinfectado com sucesso, esse objecto é restaurado para utilização regular. Se o objecto não puder ser desinfectado, então é apagado. É criada uma cópia do objecto que é armazenada na Cópia de Segurança (ver 17.2 na pág. 243).
Bloquear acesso ☐ **Desinfectar** ☑ **Apagar**	O Anti-vírus de Ficheiros bloqueará o acesso ao objecto e apagá-lo-á.

Antes de tentar desinfectar ou apagar um objecto, o Kaspersky Anti-virus para Windows Workstations cria uma cópia de segurança e envia-a para a Cópia de Segurança caso o objecto precise de ser restaurado ou surja uma oportunidade de o tratar.

7.3. Desinfecção adiada

Se seleccionar a opção **Bloquear acesso** como a acção para os programas maliciosos, os ficheiros não serão tratados e o acesso a eles será bloqueado.

E se as acções seleccionadas foram:

Bloquear acesso

Desinfectar

todos os ficheiros não tratados serão bloqueados.

Para recuperar o acesso aos ficheiros bloqueados, tem de os desinfectar. Para o fazer:

1. Seleccione o **Anti-vírus de Ficheiros** na janela principal do programa e clique com o botão esquerdo do rato em qualquer parte da caixa **Estatísticas**.
2. Seleccione os ficheiros que lhe interessam no Separador **Detectadas** e clique no botão **Acções** → **Neutralizar Todos**.

Se for desinfectado com sucesso, o ficheiro será devolvido ao utilizador. Se o ficheiro não puder ser tratado, pode *apagá-lo* ou *ignorá-lo*. No último caso, o acesso ao ficheiro será restaurado. No entanto, isto aumenta significativamente o risco de infecção no seu computador. Recomenda-se vivamente a não ignorar os ficheiros maliciosos.

CAPÍTULO 8. ANTI-VÍRUS DE E-MAIL

O Kaspersky Anti-virus para Windows Workstations inclui uma componente especial para impedir que os e-mails de entrada e de saída transfiram objectos perigosos: o Anti-vírus de E-mail. Esta componente é iniciada quando inicia o seu sistema operativo, está sempre em execução e verifica todos os e-mails com os protocolos POP3, SMTP, IMAP, MAPI[1] e NNTP, assim como ligações encriptadas (SSL) para POP3 e IMAP (SSL).

O indicador do funcionamento da componente é apresentado no ícone de bandeja do sistema do Kaspersky Anti-virus para Windows Workstations, que apresenta este aspecto sempre que um e-mail está a ser analisado.

O modo de actuação do Anti-vírus de E-mail, por defeito, é o seguinte:

1. O Anti-vírus de E-mail intercepta cada e-mail electrónico recebido ou enviado pelo utilizador.

2. O e-mail é decomposto nas suas partes: o cabeçalho do e-mail, o seu corpo e os anexos.

3. O corpo e os anexos do e-mail (incluindo anexos OLE) são verificados quanto à existência de objectos perigosos. Os objectos maliciosos são detectados, utilizando as *assinaturas de ameaças* incluídas no programa e com o algoritmo heurístico. As assinaturas contêm descrições de todos os programas maliciosos conhecidos até à data e dos métodos para os neutralizar. O algoritmo heurístico consegue detectar novos vírus que ainda não foram inseridos nas assinaturas de ameaças.

4. Depois da verificação de vírus, estão disponíveis as seguintes opções de comportamento:

    - Se o corpo ou os anexos do e-mail contiverem código malicioso, Anti-vírus de E-mail bloqueia o e-mail, coloca uma cópia do objecto infectado na cópia de segurança e vai tentar desinfectar o objecto. Se o e-mail for desinfectado com sucesso, o mesmo passa a estar novamente disponível para o utilizador. Se a desinfecção não for possível, o objecto

---

[1] As mensagens de correio electrónico a enviar com MAPI são analisadas utilizando uma extensão especial para o Microsoft Office Outlook e para o The Bat!

infectado no e-mail é apagado. Depois da verificação de vírus, é inserido um texto especial na linha de assunto do e-mail, referindo que o e-mail foi processado pelo Kaspersky Anti-virus para Windows Workstations.

- Se no corpo ou nos anexos for detectado um código que parece ser malicioso, mas não existir uma certeza absoluta, a parte suspeita do e-mail é enviada para a *Quarentena*.

- Se não for detectado qualquer código malicioso no e-mail, o mesmo é imediatamente disponibilizado ao utilizador.

É fornecida uma extensão especial (ver 8.2.2 na pág. 111) para o Microsoft Office Outlook que permite configurar, em detalhe, as análises de e-mails.

Se utilizar o The Bat!, o Kaspersky Anti-virus para Windows Workstations pode ser utilizado em conjunto com outras aplicações de anti-vírus. As regras para processar tráfego de e-mail (ver 8.2.3 na pág. 113) são configuradas directamente no The Bat! e substituem as definições de protecção de e-mail do Kaspersky Anti-virus para Windows Workstations.

Atenção!

Esta versão do Kaspersky Anti-Virus não contém extensões do Anti-vírus de E-mail para versões de 64-bit dos clientes de e-mail.

Ao trabalhar com outros programas de e-mail (incluindo o Microsoft Outlook Express (Programa de E-mail do Windows), o Mozilla Thunderbird, o Eudora, o Incredimail), o Anti-vírus de E-mail verifica e-mails com os protocolos SMTP, POP3, IMAP e NNTP.

Note que os e-mails transmitidos através do protocolo IMAP não são verificados no Thunderbird, se estiver utilizar filtros que os movem para fora da sua **Caixa de Entrada**.

8.1. Seleccionar um nível de segurança de e-mail

O Kaspersky Anti-Virus para Windows Workstations protege o seu e-mail, com um dos seguintes níveis de segurança (ver Figura 24):

Elevado – o nível com a monitorização mais abrangente dos e-mails de entrada e de saída. O programa verifica, em detalhe, os anexos de e-mails, independentemente do tempo que demorar a verificação, inclusive para arquivos.

Recomendado – Os especialistas da Kaspersky Lab recomendam este nível de segurança. Eles definem a verificação dos mesmos objectos, tal como no nível Elevado, com excepção dos anexos de e-mail que demorem mais de três minutos a verificar.

Baixo – o nível de segurança com definições que lhe permitem utilizar, de forma confortável, as aplicações que requerem mais recursos do sistema, uma vez que o conjunto de objectos de e-mail a ser verificado é menor. Assim, neste nível apenas são verificados os seus e-mails de entrada, pelo que não são verificados os arquivos e objectos (e-mails) anexados que demorem mais de três minutos a verificar. Recomenda-se que utilize este nível se estiver instalado no seu computador um software adicional de protecção de e-mail.

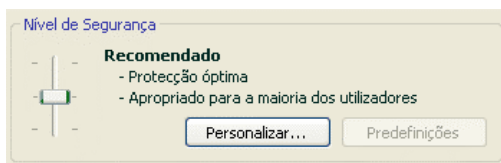



Figura 24. Escolher o nível de segurança de e-mail

Por defeito, o nível de segurança de e-mail está definido no nível **Recomendado**.

Pode aumentar ou reduzir o nível de segurança de e-mail, seleccionando o nível que deseja ou editando as definições do nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio de velocidade de verificação e o total de objectos verificados: quanto menos objectos de e-mail forem sujeitos a verificação em termos de objectos perigosos, maior é a velocidade de verificação.

Se nenhum dos níveis de segurança pré-instalados responder às suas necessidades, você pode alterar as suas definições. Se o fizer, o nível será estabelecido como **Definições Personalizadas**. Vamos examinar um exemplo de como pode ser útil ter um nível de segurança de e-mail definido pelo utilizador.

<u>Exemplo</u>:

O seu computador está fora da rede local e utiliza uma ligação à Internet através de linha telefónica. Você usa o Microsoft Outlook Express como cliente de e-mail para receber e enviar e-mails e um dos serviços de e-mail grátis como serviço de correio electrónico. Por diversas razões, o seu correio electrónico contém anexos arquivados. Como é que pode proteger o

seu computador, da melhor forma possível, relativamente a infecções através de e-mail?

Dica para a selecção de um nível de segurança:

Tendo em conta os dados disponíveis, pode-se concluir que, na situação descrita, o perigo de um programa malicioso infectar o seu computador através do e-mail é extremamente elevado (sem protecção de e-mail centralizada e o método de ligação à Internet).

Recomenda-se que utilize o nível Elevado como o seu nível de segurança básico pré-instalado, inserindo depois as seguintes alterações: aconselhamos que reduza o tempo de verificação para os anexos, por exemplo, para 1-2 minutos. A maioria dos anexos arquivados será verificada em termos de vírus e a velocidade de processamento não será seriamente reduzida.

Para modificar as definições do nível de segurança actual:

Clique no botão **Personalizar** na janela de definições do Anti-vírus de E-mail. Na janela que se abre, edite as definições de protecção de e-mail e clique em **OK**.

8.2. Configurar o Anti-vírus de E-mail

As regras segundo as quais os seus e-mails são verificados são definidas por um conjunto de definições. As definições podem ser desagregadas nos seguintes grupos:

- Definições que definem o grupo protegido de e-mails (ver 8.2.1 na pág. 109)
- Definições de análise de correio electrónico para o Microsoft Office Outlook (ver 8.2.2 na pág. 111) e o The Bat! (ver 8.2.3 na pág. 113)
- Definições que regulam as acções a tomar em relação a objectos de e-mail perigosos (ver 8.2.4 na pág. 115)

As secções que se seguem irão examinar, em detalhe, estas definições.

8.2.1. Seleccionar um grupo de e-mail protegido

O Anti-vírus de E-mail permite-lhe seleccionar, exactamente, que grupo de e-mails tem que ser verificado quanto à existência de objectos perigosos.

Por defeito, a componente protege e-mails de acordo com os parâmetros do nível de protecção **Recomendado**, o que significa verificar os e-mails de entrada e de saída. Quando começa a trabalhar com o programa, recomenda-se que verifique os e-mails de saída, uma vez que é provável que existam worms no seu computador que utilizam o e-mail como um canal para se distribuírem. Isto ajudará a evitar situações indesejáveis relacionadas com o envio em massa e não motorizado de e-mails infectados a partir do seu computador.

Se tiver a certeza de que os e-mails que está a enviar não podem conter objectos perigosos, você pode desactivar a verificação de e-mails de saída. Para o fazer:

1. Seleccione o **Anti-vírus de E-mail** na janela principal e aceda à janela de definições da componente, clicando em Definições. Clique no botão **Personalizar** na janela de configuração do Anti-vírus de E-mail.

2. Na janela **Definições Personalizadas: Anti-vírus de E-mail** (ver Figura 25), seleccione a opção **Apenas e-mails de entrada** que é apresentada na secção **Âmbito**.

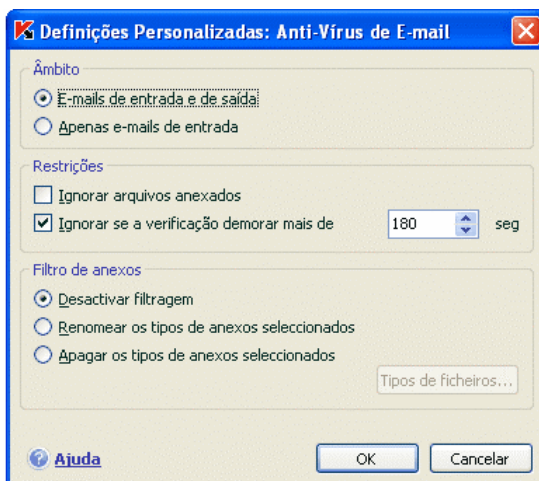



Figura 25. Definições do Anti-vírus de E-mail

Para além de seleccionar um grupo de e-mail, você pode especificar se os anexos arquivados devem ser verificados e também definir o período de tempo máximo para a verificação de um objecto de e-mail. Estas definições são configuradas na secção **Restrições**.

Se o seu computador não está protegido por nenhum software de rede local e o seu acesso à Internet não envolve nenhum servidor de proxy ou firewall,

recomenda-se que não desactive a verificação de anexos arquivados e que não defina um limite de tempo para a verificação.

Se está a trabalhar num ambiente protegido, você pode alterar as restrições do tempo de verificação para aumentar a velocidade de verificação de e-mails.

Pode configurar as condições de filtragem para os objectos associados a uma mensagem de e-mail na secção **Filtro de anexos**:

- **Desactivar filtragem** – não utiliza a filtragem adicional para anexos.
- **Renomear os tipos de anexos seleccionados** – descarta um determinado formato de anexo e substitui o último caractere do nome do ficheiro por um traço inferior (underscore). Pode seleccionar os tipos de ficheiros, clicando no botão **Tipos de ficheiros**.
- **Apagar os tipos de anexos seleccionados** – descarta e apaga determinado formato de anexo. Pode seleccionar os tipos de ficheiros, clicando no botão **Tipos de ficheiros**.

Pode encontrar mais informação sobre a filtragem de tipos de anexos na secção A.1 na pág. 329.

Ao utilizar o filtro, você adiciona segurança ao seu computador, uma vez que os programas maliciosos espalham-se através de e-mails e, mais frequentemente, enquanto anexos. Ao renomear ou apagar determinados tipos de anexos, você protege o seu computador, evitando que este abra anexos, automaticamente, quando é recebida uma mensagem e outros perigos potenciais.

8.2.2. Configurar o processamento de e-mails no Microsoft Office Outlook

Se utiliza o Microsoft Outlook como o seu cliente de e-mail, pode definir configurações personalizadas para as verificações de vírus.

Quando instala o Kaspersky Anti-virus para Windows Workstations, é instalada uma extensão especial (plug-in) no Microsoft Office Outlook. Este plug-in consegue rapidamente apresentar a configuração das definições do Anti-vírus de E-mail e ainda determinar a que horas o e-mail será verificado quanto à existência de vírus.

Aviso!

Esta versão do Kaspersky Anti-virus não contém plug-ins do Anti-vírus de E-mail para o Microsoft Office Outlook 64-bit.

A extensão vem sob a forma de um separador especial: **Anti-vírus de E-mail**, localizado em **Serviço** → **Opções** (ver Figura 26).

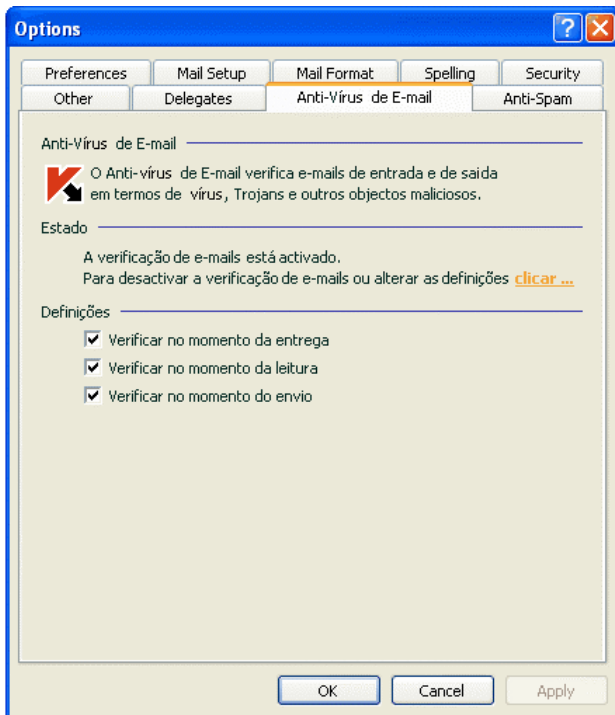



Figura 26. Configurar as definições do Anti-vírus de E-mail no Microsoft Outlook

Seleccione um modo de análise do correio electrónico:

- ☑ **Verificar no momento da entrega** – analisa cada e-mail no momento em que este entra na sua caixa de entrada.
- ☑ **Verificar no momento da leitura** – verifica o e-mail quando você o abrir para o ler**.**
- ☑ **Verificar no momento do envio** – analisa cada e-mail que envia, quando à existência de vírus, no momento em que o envia.

Aviso!

Se utiliza uma ligação ao seu serviço de e-mail do Microsoft Office Outlook, através do protocolo IMAP, recomenda-se que não utilize o modo **Verificar no momento da entrega**. Ao activar este modo, fará com que os e-mails sejam copiados para o seu computador local quando forem entregues ao servidor e, por conseguinte, a principal vantagem do IMAP é perdida -- criar menos tráfego e lidar com e-mails indesejados no servidor, sem os copiar para o computador do utilizador.

A acção que será executada em relação aos objectos de e-mail perigosos é definida nas definições do Anti-vírus de E-mail, que podem ser configuradas seguindo a ligação clique aqui na secção **Estado**.

8.2.3. Configurar as verificações de e-mails no The Bat!

No programa The Bat!, as acções executadas sobre objectos de e-mail infectados são definidas com as ferramentas do próprio programa.

> Aviso!
>
> As definições do Anti-vírus de E-mail são ignoradas, especificamente as definições que determinam se os e-mails de entrada ou de saída são verificados, assim como as acções a executar sobre objectos de e-mail perigosos e as exclusões. As únicas definições que o The Bat! toma em consideração estão relacionadas com a verificação de anexos arquivados e os limites de tempo na verificação de e-mails (ver 8.2.1 na pág. 109).
>
> Esta versão do Kaspersky Anti-Virus não fornece plug-ins do Anti-vírus de E-mail para a versão 64-bit do The Bat!.

Para configurar as regras de protecção de e-mail no The Bat!:

1. Seleccione **Settings (Definições)** no menu **Properties (Propriedades)**.
2. Seleccione **Virus protection (Protecção de vírus)** na árvore de definições.

As definições de protecção indicadas (ver Figura 27) abrangem todos os módulos de anti-vírus instalados no computador e que apoiam o trabalho efectuado com o The Bat!.

Tem que decidir:

- Que grupo de e-mails será sujeito a verificações de vírus (e-mails de entrada, e-mails de saída);
- Em que altura os objectos de e-mail serão verificados, quanto à existência de vírus (quando abrir um e-mail ou antes de salvar um e-mail no disco);
- As acções executadas pelo cliente de e-mail quando são detectados objectos perigosos em e-mails. Por exemplo, você poderia seleccionar:

  Attempt to disinfect infect parts (Tentar desinfectar partes infectadas) – tenta tratar o objecto de e-mail infectado e se o

objecto não puder ser desinfectado, o mesmo permanece no e-mail. O Kaspersky Anti-virus para Windows Workstations irá sempre informá-lo que o objecto de e-mail está infectado. Mas mesmo que seleccione a opção **Apagar** na janela de aviso do Anti-vírus de E-mail, o objecto permanecerá no e-mail, uma vez que a acção seleccionada no The Bat! tem prioridade sobre as acções do Anti-vírus de E-mail.

Delete infected parts (Apagar partes infectadas) – apaga o objecto perigoso do e-mail, independentemente do objecto estar infectado ou se suspeitar de estar infectado.

Por defeito, o The Bat! coloca na pasta da Quarentena todos os objectos de e-mail infectados, sem os tratar.

> Aviso!
>
> O The Bat! não cria cabeçalhos especiais para os e-mails que contêm objectos perigosos.

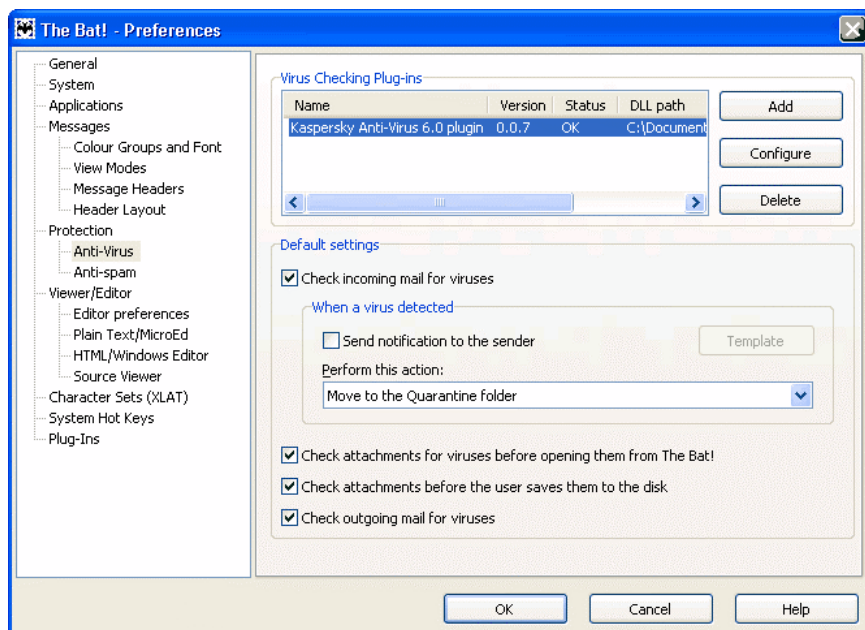



Figura 27. Configuração das análises de e-mails no The Bat!

8.2.4. Restaurar as predefinições do Anti-vírus de E-mail

Quando configura o Anti-vírus de E-mail, pode sempre regressar às definições de desempenho recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as com o nível de segurança **Recomendado**.

Para restaurar as predefinições do Anti-vírus de E-mail:

1. Seleccione o **Anti-vírus de E-mail** na janela principal e aceda à janela de definições da componente, clicando em Definições.
2. Clique no botão **Predefinições** na secção **Nível de Segurança**.

8.2.5. Seleccionar acções para objectos de e-mail perigosos

Quando, ao verificar um e-mail quanto à existência de vírus, se descobrir que o e-mail ou qualquer uma das suas partes (cabeçalho, corpo, anexo) está infectado ou se suspeitar que está infectado, as operações subsequentes do Anti-vírus de E-mail dependem do estado do objecto e da acção seleccionada.

Após a verificação, um objecto de e-mail pode ser classificado com um dos seguintes estados:

- *Programa malicioso* (vírus, Trojan) – para mais detalhes, ver 1.1 na pág. 11).
- *Potencialmente infectado*, quando a verificação não consegue determinar se o objecto está infectado. Isto significa que o código do ficheiro contém uma secção de código que se assemelha a um vírus conhecido mas alterado ou que faz lembrar a estrutura de uma sequência de vírus.

Por defeito, quando é detectado um objecto perigoso ou suspeito, o **Anti-vírus de E-mail** exibe um aviso no ecrã e dá-lhe à escolha diversas acções para o objecto.

Para editar uma acção para um objecto:

Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations e seleccione o **Anti-vírus de E-mail**. Todas as acções passíveis para objectos perigosos estão listadas na caixa **Acção** (ver Figura 28).

Figura 28. Seleccionar acções para ficheiros de correio electrónico perigosos

Vejamos, mais detalhadamente, as opções possíveis para processar ficheiros perigosos de mensagens de correio electrónico.

Se a acção seleccionada foi	Quando é detectado um objecto perigoso
Perguntar o que fazer	O Anti-vírus de E-mail exibirá uma mensagem de aviso que contém informação sobre qual o programa malicioso que infectou (infectou potencialmente) o ficheiro e dá-lhe à escolha uma das seguintes acções.
Bloquear acesso	O Anti-vírus de E-mail bloqueará o acesso ao objecto. A informação acerca disto é gravada no relatório (ver 17.3 na pág. 245). Pode tentar desinfectar este objecto mais tarde.

Se a acção seleccionada foi	Quando é detectado um objecto perigoso
Bloquear acesso Desinfectar	O Anti-vírus de E-mail bloqueará o acesso ao objecto e tentará desinfectá-lo. Se for desinfectado com sucesso, esse objecto será restaurado para uso normal. Se o objecto não puder ser tratado, este será movido para a Quarentena (ver 17.1 na pág. 239). A informação acerca disto é gravada no relatório. Mais tarde, você pode tentar desinfectar este objecto.
Bloquear acesso Desinfectar Apagar se a desinfecção falhar[2]	O Anti-vírus de E-mail bloqueará o acesso ao objecto e tentará desinfectá-lo. Se for desinfectado com sucesso, esse objecto será restaurado para uso normal. Se o objecto não puder ser desinfectado, o mesmo será apagado. Será guardada uma cópia do objecto na Cópia de Segurança. Os objectos com o estado *potencialmente infectado* serão movidos para a Quarentena.
Bloquear acesso Desinfectar Apagar	Quando o Anti-vírus de E-mail detecta um objecto infectado ou potencialmente infectado, esse objecto é apagado sem informar o utilizador.

Ao desinfectar ou apagar um objecto, o Kaspersky Anti-virus para Windows Workstations cria uma cópia de segurança e envia-a para a Cópia de Segurança (ver 17.2 na pág. 243) antes de tentar tratar o objecto o apagá-lo, caso o objecto precise de ser restaurado ou surja uma oportunidade de o tratar.

---

[2] Se utilizar o The Bat! como cliente de e-mail e esta acção do Anti-vírus de E-mail for aplicada, os objectos perigosos serão ou desinfectados ou apagados (dependendo do tipo de acção seleccionada no programa The Bat!).

CAPÍTULO 9. ANTI-VÍRUS DE INTERNET

Sempre que utiliza a Internet, você está a submeter a informação armazenada no seu computador ao risco de infecção por programas perigosos. Estes programas podem ser carregados no seu computador quando abre um site ou lê um artigo na Internet.

O Kaspersky Anti-virus para Windows Workstations inclui uma componente especial para garantir a segurança da sua utilização da Internet: o *Anti-vírus de Internet*. Esta componente protege a informação que entra no seu computador através de HTTP e também impede que sejam carregados scripts perigosos no computador.

> Aviso!
>
> O Anti-vírus de Internet apenas monitoriza o tráfego de http que passa através das portas listadas na lista de portas monitorizadas (ver 17.7 na pág. 267). Está incluída no pacote do programa uma lista das portas que são mais frequentemente utilizadas para transmitir tráfego de e-mails e de HTTP. Se utiliza portas que não estão nesta lista, adicione-as para proteger o tráfego efectuado através das mesmas.

Se está a trabalhar num espaço desprotegido, acedendo à Internet através de um modem, recomenda-se que utilize o Anti-vírus de Internet para se proteger enquanto utiliza a Internet. Se o seu computador está a funcionar numa rede protegida por uma firewall ou filtros de tráfego de HTTP, o Anti-vírus de Internet fornece-lhe protecção adicional na utilização da Internet.

O indicador do funcionamento da componente é apresentado no ícone de bandeja do sistema do Kaspersky Anti-virus para Windows Workstations, que apresenta este aspecto sempre que os scripts estão a ser verificados.

Vejamos, mais detalhadamente, o esquema de funcionamento da componente.

O Anti-vírus de Internet consiste em dois módulos que lidam com:

- *Verificação de tráfego* – a verificação de objectos que entram no computador do utilizador através de HTTP.
- *Verificação do Navegador de Internet* – verificação de todos os scripts processados no Microsoft Internet Explorer, assim como todos os scripts WSH (JavaScript, Visual Basic Script, etc.) que são carregados enquanto o utilizador está a utilizar o computador.

Uma extensão especial é fornecida para o Microsoft Internet Explorer que é instalada quando o Kaspersky Anti-virus para Windows Workstations é

instalado. O ícone no painel de ferramentas do navegador indica-lhe que a mesma está instalada. Se clicar no ícone é aberto um painel de informação com as estatísticas do Anti-vírus de Internet sobre o número de scripts verificados e bloqueados.

O Anti-vírus de Internet protege o tráfego HTTP da seguinte forma:

1. Cada página de Internet ou ficheiro que é acedido pelo utilizador ou por um determinado programa, através de HTTP, é interceptado e analisado pelo Anti-vírus de Internet, quanto à existência de código malicioso. Os objectos maliciosos são detectados, utilizando as assinaturas de ameaças incluídas no Kaspersky Anti-virus para Windows Workstations e com o algoritmo heurístico. As assinaturas contêm descrições de todos os programas maliciosos conhecidos até à data e dos métodos para os neutralizar. O algoritmo heurístico consegue detectar novos vírus que ainda não foram inseridos nas assinaturas de ameaças.

2. Depois da análise, estão disponíveis as seguintes opções de comportamento:

   a. Se a página de Internet ou objecto, aos quais o utilizador está a tentar aceder, contiverem código malicioso, o programa bloqueia o acesso aos mesmos. Depois, surge uma mensagem no ecrã, referindo que o objecto ou a página estão infectados.

   b. Se o ficheiro ou a página de Internet não contiverem código malicioso, de imediato, o programa concede ao utilizador o acesso aos mesmos.

Os scripts são analisados de acordo com o seguinte algoritmo:

1. Cada script, executado numa página de Internet, é interceptado pelo Anti-vírus de Internet e é analisado quanto à presença de código malicioso.

2. Se o script contiver código malicioso, o Anti-vírus de Internet bloqueia o acesso ao mesmo e informa o utilizador através de uma mensagem especial que surge no ecrã.

3. Se não for detectado qualquer código malicioso no script, o mesmo é executado.

> Aviso!
>
> O Anti-vírus de Internet deve estar activado antes de estabelecer a ligação à origem na Internet, a fim de poder interceptar e verificar o tráfego http e scripts para ver se contêm vírus ou não.

9.1. Seleccionar um nível de segurança da Internet

O Kaspersky Anti-Virus para Windows Workstations protege o seu computador, enquanto utiliza a Internet, com um dos seguintes níveis de segurança (ver Figura 29):

Elevado – o nível com a monitorização mais abrangente dos scripts e objectos que entram no seu computador através de HTTP. O programa executa uma verificação exaustiva de todos os objectos, utilizando o conjunto completo das assinaturas de ameaças. Este nível de segurança é recomendado para ambientes agressivos, quando não estão a ser utilizadas outras ferramentas de protecção do tráfego de HTTP.

Recomendado – as definições deste nível são recomendadas pelos especialistas da Kaspersky Lab. Este nível analisa os mesmos objectos que o nível **Elevado**, mas limita o tempo de memória temporária para fragmentos de ficheiros, acelerando assim a verificação e devolvendo, mais rapidamente, os objectos ao utilizador.

Baixo – nível de segurança com definições que lhe permitem utilizar, de forma confortável, as aplicações que requerem mais recursos do sistema, uma vez que o âmbito de objectos verificados é reduzido, utilizando um conjunto limitado das assinaturas de ameaças. Recomenda-se que seleccione este nível de protecção, se estiver instalado no seu computador um software adicional de protecção da Internet.

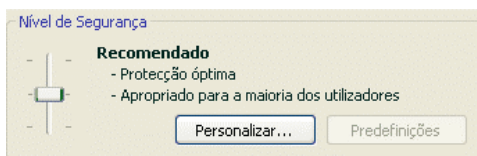



Figura 29. Seleccionar um nível de segurança para a Internet

Por defeito, o Anti-vírus de Internet está definido no nível **Recomendado**.

Pode aumentar ou baixar o nível de protecção, seleccionando o nível que pretende ou alterando as definições do nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio de velocidade de verificação e o total de objectos verificados:

quanto menos objectos forem sujeitos a análise, quanto à presença de objectos perigosos, maior é a velocidade de verificação.

Se um nível de segurança pré-estabelecido não responder às suas necessidades, você pode criar um nível de segurança com **Definições Personalizadas**. Vamos examinar um exemplo de como pode ser útil ter um nível de segurança definido pelo utilizador.

Exemplo:

O seu computador liga-se à Internet através de um modem. O computador não está integrado na Rede de Área Local da empresa e não tem qualquer protecção anti-vírus, no que respeita ao tráfego de HTTP que entra no seu computador.

Devido à natureza do seu trabalho, regularmente, você transfere ficheiros extensos a partir da Internet. A verificação de ficheiros como esses, por regra, requer grandes quantidades de tempo.

Como é que pode proteger o seu computador, da melhor forma possível, relativamente a infecções através de tráfego de HTTP ou de scripts?

Dica para seleccionar um nível de segurança:

Tendo em conta os dados disponíveis, pode-se concluir que o seu computador está a funcionar num ambiente agressivo e o perigo de um programa malicioso infectar o seu computador, através de tráfego de HTTP, é extremamente elevado (não dispõe de um anti-vírus de Internet centralizado e o método de ligação à Internet).

Recomenda-se que utilize o nível **Elevado** como o seu nível de segurança básico pré-instalado, inserindo depois as seguintes alterações: aconselhamos que limite o tempo de memória temporária para fragmentos de ficheiros durante a verificação.

Para modificar um nível de segurança pré-instalado:

Clique no botão **Personalizar** na janela de definições do Anti-Vírus de Internet. Na janela que se abre, edite as definições (ver 9.2 na pág. 121) e clique em **OK**.

9.2. Configurar o Anti-vírus de Internet

O Anti-vírus de Internet verifica todos os objectos que são carregados no seu computador através do protocolo HTTP e monitoriza todos os scripts WSH (Scripts de Java, Visual Basic, etc.) executados no computador.

Você pode configurar algumas definições do Anti-vírus de Internet, no sentido de aumentar a velocidade de funcionamento da componente, especificamente:

- Definir o algoritmo de verificação, seleccionando um conjunto completo ou limitado das assinaturas de ameaças
- Criar uma lista de endereços de confiáveis

Para além disso, pode seleccionar as acções a executar em relação a objectos de HTTP perigosos.

As secções que se seguem irão examinar, em detalhe, estas definições.

9.2.1. Definir um método de verificação

Pode verificar os dados transferidos da Internet, utilizando um dos seguintes métodos:

- *Verificação de transmissão contínua* - tecnologia de detecção de código malicioso no tráfego de rede, que verifica os dados de forma instantânea. Por exemplo, você está a transferir um ficheiro da Internet. O Anti-vírus de Internet verifica o ficheiro, à medida que você transfere partes do mesmo para o seu computador. Esta tecnologia disponibiliza o objecto verificado ao utilizador, de forma mais rápida. Ao mesmo tempo, é utilizado um conjunto limitado das assinaturas de ameaças para efectuar as verificações de transmissão contínua (apenas as ameaças mais activas), o que reduz, significativamente, o nível de segurança da utilização da Internet.
- *Verificação de armazenamento temporário* - tecnologia de detecção de código malicioso no tráfego de rede, que verifica os objectos depois destes terem sido, completamente, transferidos para a memória intermédia. Depois disso, o objecto é analisado em termos de vírus e, de acordo com os resultados obtidos, o programa devolve o objecto ao utilizador ou bloqueia-o.
  Quando utilizar este tipo de verificação, é utilizado o conjunto completo das assinaturas de ameaças, o que pode aumentar o nível de detecção de código malicioso. Contudo, a utilização deste método aumenta o tempo de processamento do objecto e o tempo decorrido antes do programa devolver os objectos ao utilizador. Adicionalmente, também pode causar problemas ao copiar ou processar objectos extensos, uma vez que é excedido o tempo limite na ligação ao cliente de http.

Para seleccionar o método de verificação que o Anti-vírus de Internet irá utilizar:

1. Clique no botão **Personalizar** na janela de configuração do Anti-vírus de Internet.

2. Na janela que se abre (ver Figura 30), seleccione a opção que deseja na secção **Método de verificação**.

Por defeito, o Anti-vírus de Internet verifica os dados transferidos a partir da Internet, através da memória intermédia e utiliza o conjunto completo das assinaturas de ameaças.

> Aviso!
>
> Se tiver problemas de acesso quando utilizar recursos como rádio pela Internet, vídeos de transmissão contínua, ou conferências pela Internet, utilize a verificação de transmissão contínua.

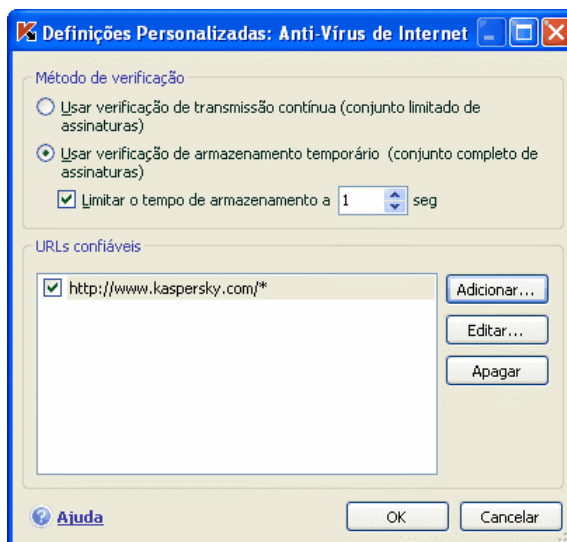



Figura 30. Configurar o Anti-Vírus de Internet

9.2.2. Criar uma lista de endereços confiáveis

Tem a opção de criar uma lista de endereços confiáveis, em cujos conteúdos você confia incondicionalmente. O Anti-vírus de Internet não analisará os dados desses endereços, quanto à existência de objectos perigosos. Esta opção pode ser utilizada nos casos em que o Anti-vírus de Internet interfere com a transferência de um determinado ficheiro, bloqueando uma tentativa para transferi-lo.

Para criar uma lista de endereços confiáveis:

1. Clique no botão **Personalizar** na janela de configuração do Anti-Vírus de Internet.
2. Na janela que se abre (ver Figura 30), crie uma lista de servidores confiáveis na secção **URLs confiáveis**. Para o fazer, utilize os botões apresentados à direita da lista.

Quando inserir um endereço confiável, você pode criar máscaras com os seguintes símbolos especiais:

***** – qualquer combinação de caracteres.
Exemplo: Exemplo: Se criar a máscara ***abc***, não será verificado nenhum URL que contenha abc. Por exemplo:
www.virus.com/download_virus/page_0-9abcdef.html

? – qualquer símbolo único.
Exemplo: Se criar a máscara **Patch_123?.com**, não serão verificados os URLs que contenham aquela série de caracteres e mais um caractere qualquer a seguir ao 3. Por exemplo: **Patch_12345.com.** Contudo, o endereço **patch_1234.com** será verificado.

Se um * ou um ? fizer parte do próprio URL que é adicionado à lista, quando os inserir, deve usar uma barra invertida (\) para ignorar o asterisco ou o ponto de interrogação que surge a seguir a essa barra.

Exemplo: Quer adicionar o seguinte URL à lista de endereços confiáveis: www.virus.com/download_virus/virus.dll?virus_name=

Para que o Kaspersky Anti-virus para Windows Workstations não processe o ? como um metacaractere, você insere uma barra invertida à frente do mesmo. Assim, o URL que está a adicionar à lista de exclusões será o seguinte:

www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Restaurar as predefinições do Anti-vírus de Internet

Quando configura o Anti-vírus de Internet, pode sempre regressar às definições de desempenho recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as com o nível de segurança **Recomendado**.

Para restaurar as predefinições do Anti-Vírus de Internet:

1. Seleccione o **Anti-Vírus de Internet** na janela principal e aceda à janela de definições da componente, clicando em Definições.
2. Clique no botão **Predefinições** na secção **Nível de Segurança**.

9.2.4. Seleccionar acções para objectos perigosos

Quando, ao verificar um objecto de HTTP, se descobrir que o mesmo contém código malicioso, as operações subsequentes do Anti-vírus de Internet dependem da acção que seleccionar.

Para configurar as reacções do Anti-vírus de Internet em relação a objectos perigosos:

Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations e seleccione o **Anti-Vírus de Internet**. Na secção **Acção** estão listadas todas as acções possíveis para ficheiros perigosos (ver Figura 31).

Por defeito, quando é detectado um objecto de http perigoso, o Anti-vírus de Internet exibe uma mensagem de aviso no ecrã e dá-lhe à escolha várias acções para o objecto.

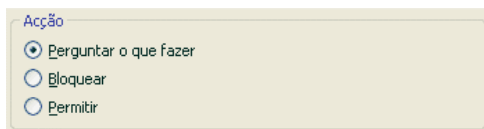



Figura 31. Seleccionar acções para scripts perigosos

As opções possíveis para processar objectos de HTTP perigosos são as seguintes:

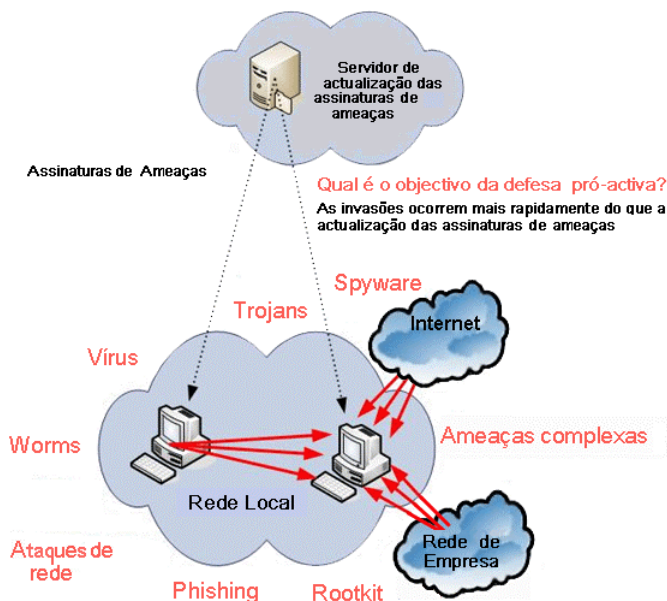
Se a acção seleccionada foi	Quando é detectado um objecto perigoso no tráfego de HTTP
Perguntar o que fazer	O Anti-vírus de Internet exibirá uma mensagem de aviso que contém informação sobre qual o código malicioso que infectou potencialmente o objecto e dá-lhe à escolha uma das seguintes acções.
Bloquear	O Anti-vírus de Internet bloqueará o acesso ao objecto e exibirá uma mensagem no ecrã acerca desse bloqueio. A informação acerca disto será gravada no relatório (ver 17.3 na pág. 245).

Se a acção seleccionada foi	Quando é detectado um objecto perigoso no tráfego de HTTP
Permitir	O Anti-vírus de Internet permitirá o acesso ao objecto. A informação acerca disto será gravada no relatório.

O Anti-vírus de Internet bloqueia sempre os scripts perigosos e emite mensagens que informam o utilizador sobre a acção executada. Você não pode alterar a acção executada em relação a scripts perigosos, para além da opção de desactivar o módulo de verificação de scripts.

CAPÍTULO 10. DEFESA PRÓ-ACTIVA

Aviso!
Nesta versão da aplicação não existe a componente de Defesa Pró-activa (**Monitorização de Macros VBA**) para computadores com o Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou com o Microsoft Windows Vista x64.

O Kaspersky Anti-Virus para Windows Workstations protege o seu computador em relação a ameaças conhecidas e ameaças novas, sobre as quais não existe informação nas assinaturas de ameaças. Isto é assegurado por uma componente especialmente desenvolvida para esse efeito: a *Defesa pró-activa.*

A necessidade de Defesa pró-activa tem aumentado, à medida que os programas maliciosos se começaram a espalhar mais depressa do que a distribuição de actualizações de anti-vírus para os neutralizar.

A técnica reactiva, na qual se baseia a protecção anti-vírus, implica que uma nova ameaça infecte pelo menos um computador e requer tempo para analisar o código malicioso, adicioná-lo às assinaturas de ameaças e actualizar esta base

de dados nos computadores dos utilizadores. Na altura em que se termina esse processo, já a nova ameaça terá incorrido em danos significativos.

As tecnologias preventivas, nas quais se baseia a Defesa pró-activa do Kaspersky Anti-virus para Windows Workstations, podem evitar a perda de tempo e neutralizar novas ameaças antes destas terem danificado o seu computador. Como é que isso é feito? Em contraste com as tecnologias reactivas, que analisam código através das assinaturas de ameaças, as tecnologias preventivas reconhecem uma nova ameaça no seu computador, através de uma sequência de acções executadas por um determinado programa. A aplicação inclui um conjunto de critérios definidos que podem ajudar a determinar se a actividade de um programa é perigosa ou não. Se a análise da actividade mostra que as acções de um determinado programa são suspeitas, o Kaspersky Anti-virus executará a acção atribuída pela regra para aquele tipo de actividade específica.

A actividade perigosa é determinada pelas acções global do programa. Por exemplo, quando se detectam acções como sejam um programa a copiar-se para os recursos de rede, a pasta de arranque ou o registo do sistema e depois a enviar cópias de si próprio, é muito provável que este programa seja um worm (verme). O comportamento perigoso também inclui:

- alterações ao sistema de ficheiros
- módulos a serem incorporados noutros processos
- dissimulação de processos (máscaras)
- alterações às chaves de registo do sistema Microsoft Windows

A Defesa pró-activa localiza e bloqueia todas as operações perigosas, utilizando o conjunto de regras juntamente com uma lista de aplicações excluídos. A Defesa pró-activa também detecta todas as macros executadas em aplicações do Microsoft Office.

A Defesa pró-activa utiliza um conjunto de regras incluídas na aplicação, assim como regras criadas pelo utilizador ao utilizar a aplicação. Uma *regra* é um conjunto de critérios que definem o comportamento suspeito e a forma como o Kaspersky Anti-Virus reage ao mesmo.

São fornecidas regras individuais para a actividade da aplicação e para a monitorização de alterações ao registo do sistema, macros e processos em execução no computador. Mais tarde, pode alterar a lista de regras ao seu critério, adicionando, apagando ou editando-as. As regras podem bloquear acções ou conceder permissões.

Examinemos os algoritmos da Defesa Pró-activa:

1. Imediatamente após o computador ser iniciado, a Defesa pró-activa analisa os seguintes factores:

- *As acções de cada aplicação em execução no seu computador.* A Defesa pró-activa grava um histórico de acções executadas e compara-as com sequências características de uma actividade perigosa (uma base de dados sobre tipos de actividades perigosas é fornecida com o programa e actualizada com as assinaturas de ameaças).
- *As acções de cada macro VBA executada.* O programa verifica essas acções, comparando-as com a lista de acções perigosas incluída no programa.
- *Cada tentativa para editar o registo do sistema,* apagando ou adicionando chaves de registo do sistema, inserindo valores estranhos para chaves, etc.

2. A análise é conduzida, utilizando regras de *permissão* (de acordo com critérios relevantes, o comportamento é seguro) e de *bloqueio* (de acordo com critérios relevantes, o comportamento é malicioso) da Defesa Pró-activa.
3. Depois da análise, estão disponíveis as seguintes opções de comportamento:
   - Se a actividade não for considerada como perigosa com base nos critérios relevantes (regras de *permissão* e de *bloqueio*), esta actividade é permitida.
   - Se a actividade for considerada como perigosa com base nos critérios relevantes, os passos subsequentemente executados pela componente correspondem às instruções especificadas na regra: tal actividade é normalmente bloqueada. Será exibida uma mensagem no ecrã, especificando o programa perigoso, o seu tipo de actividade e um histórico das acções executadas. Você tem que aceitar a decisão por si próprio: bloquear ou permitir esta actividade. Você pode criar uma regra para essa actividade e reverter as acções executadas no sistema.

10.1. Definições da Defesa Pró-activa

As categorias de definições (ver Figura 32) para a componente Defesa pró-activa são:

- *Se a actividade das aplicações é sujeita a monitorização no seu computador*

Este modo da Defesa Pró-activa é controlado pela opção ☑ **Activar Analisador da Actividade das Aplicações**. Por defeito, este modo está activado, garantindo que as acções de quaisquer programas abertos no seu computador serão analisadas com atenção. É destacado um conjunto de actividades perigosas, para cada uma das quais você pode configurar o procedimento de processamento das aplicações para aquela actividade (ver 10.1.1 na pág. 131). Também pode criar exclusões para a Defesa pró-activa, com as quais você pode impedir que seja monitorizada a actividade das aplicações seleccionadas.

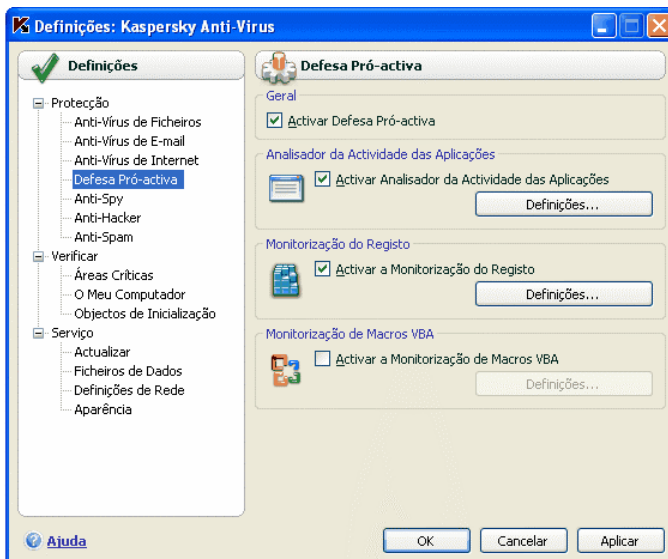



Figura 32. Definições da Defesa Pró-activa

- *Se as alterações do registo do sistema são monitorizadas*

Por defeito, a caixa ☑ **Activar a Monitorização do Registo** está assinalada, o que significa que o Kaspersky Anti-virus para Windows Workstations analisa, cuidadosamente, todas as tentativas de alteração das chaves de registo do sistema operativo.

Pode criar as suas próprias regras (ver 10.1.3.2 na pág. 140) para monitorizar o registo, dependendo da chave de registo do Microsoft Windows.

- *Se as macros são verificadas*

  A monitorização de Macros Visual Basic for Applications no seu computador é controlada assinalando a caixa **Activar a Monitorização de Macros VBA**. Por defeito, esta caixa está assinalada.

  Pode seleccionar quais as macros que são consideradas perigosas e o que fazer em relação às mesmas (ver 10.1.2 na pág. 135).

  Esta componente da Defesa Pró-activa não está disponível para o Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou Microsoft Windows Vista x64.

Pode configurar exclusões (ver 6.3.1 na pág. 78) para os módulos da Defesa Pró-activa e criar uma lista de aplicações confiáveis (ver 6.3.2 na pág. 83).

As secções que se seguem irão examinar, em detalhe, estes aspectos.

10.1.1. Regras de controlo de actividades

Note que a configuração do controlo de aplicações com o Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou Microsoft Windows Vista x64 difere do processo de configuração noutros sistemas operativos.

No final desta secção, é fornecida informação sobre como configurar o controlo de actividades para estes sistemas operativos.

O Kaspersky Anti-virus monitoriza a actividades das aplicações no seu computador. A aplicação inclui um conjunto de descrições de eventos que podem ser registados como perigosos. É criada uma regra de monitorização para cada um desses eventos. Se a actividade de qualquer aplicação for classificada como um evento perigoso, a Defesa pró-activa irá seguir, de forma estrita, as instruções referidas na regra para aquele evento.

Seleccione a caixa **Activar Analisador da Actividade das Aplicações** se desejar monitorizar a actividade das aplicações.

Vejamos vários tipos de eventos que ocorrem no sistema e que a aplicação irá registar como suspeitos:

- *Comportamento perigoso.* O Kaspersky Anti-virus analisa a actividade das aplicações instaladas no seu computador e detecta actividades perigosas ou suspeitas, com base na lista de regras criadas pela Kaspersky Lab, detecta acções perigosas ou suspeitas por parte dos programas. Tais acções incluem, por exemplo, instalação dissimulada de programas ou programas a copiarem-se a eles próprios.

- *Execução do navegador de Internet com parâmetros.* Ao analisar este tipo de actividade, você pode detectar tentativas para abrir um navegador com definições. Esta actividade é característica das situações em que o navegador de Internet é aberto a partir de uma aplicação com determinadas definições de comando de execução imediata: por exemplo, esta acção é executada se você clicar numa ligação para um determinado URL contida num e-mail de publicidade..

- *Intrusão em processos (invasores)* – adicionar código executável ou criar um fluxo adicional para o processo de um determinado programa. Esta actividade é, amplamente, utilizada por Trojans.

- *Processos Ocultos (rootkit)*. Um rootkit (processo oculto) é um conjunto de programas usados para mascarar programas maliciosos e os seus processos no sistema. O Kaspersky Anti-virus analisa o sistema operativo quanto à presença de processos dissimulados.

- *Ganchos em janelas (window hooks)*. Esta actividade é utilizada em tentativas para ler passwords e outras informações confidenciais apresentadas nas caixas de diálogo do sistema operativo. O Kaspersky Anti-Virus detecta esta actividade se forem feitas tentativas para interceptar os dados transferidos entre o sistema operativo e a caixa de diálogo.

- *Valores suspeitos no registo*. O registo do sistema é a base de dados para armazenar definições do sistema e do utilizador, que controlam o funcionamento do Windows, assim como quaisquer utilitários estabelecidos no computador. Os programas maliciosos, ao tentarem mascarar a sua presença no sistema, copiam valores incorrectos nas chaves de registo. O Kaspersky Anti-virus analisa as entradas no registo do sistema quanto à presença de valores suspeitos.

- *Actividades de sistema suspeitas*. O programa analisa as acções executadas pelo Microsoft Windows e detecta actividades suspeitas. Um exemplo de actividade suspeita seria uma violação da integridade, que envolve alterar um ou vários módulos numa aplicação monitorizada desde que foi executada pela última vez.

- *Detecção de registadores de teclas digitadas*. Esta actividade é utilizada em tentativas, por parte de programas maliciosos, para ler passwords e outras informações confidenciais que você inseriu com o seu teclado.

- *Protecção do Gestor de Tarefas do Microsoft Windows*. O Kaspersky Anti-virus protege o Gestor de Tarefas em relação a módulos maliciosos que se tentar inserir no gestor no sentido de bloquear o funcionamento do Gestor de Tarefas.

A lista de actividades perigosas é automaticamente adicionada quando o Kaspersky Anti-virus para Windows Workstations é actualizado e não pode ser editada. Você pode:

- Desligar a monitorização de uma actividade ou outra, desmarcando a caixa ☑ que aparece junto ao respectivo nome
- Editar a regra que a Defesa Pró-activa utiliza quando detecta uma actividade perigosa
- Criar uma lista de exclusões (ver 6.3 na pág. 77) listando as aplicações que você não considera perigosas.

Para configurar a monitorização de actividades,

1. Abra a janela de opções do Kaspersky Anti-virus para Windows Workstations clicando em Definições na janela principal do programa.
2. Seleccione a **Defesa Pró-activa** na árvore de definições.
3. Clique no botão **Definições** na secção **Activar Analisador da Actividade das Aplicações**.

Os tipos de actividade que a Defesa Pró-activa monitoriza estão listados na janela **Definições**: **Analisador da Actividade das Aplicações** (ver Figura 33).

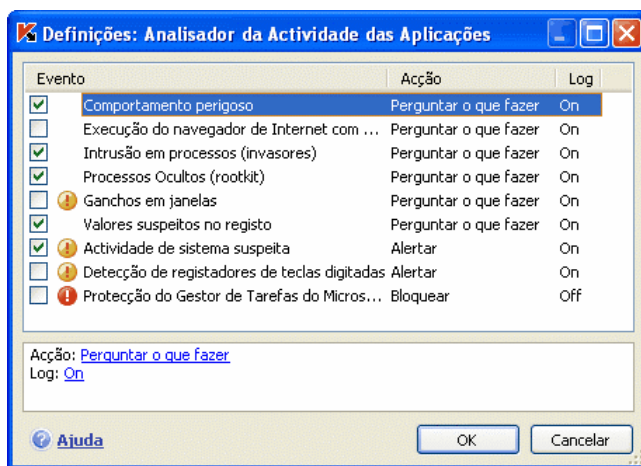



Figura 33. Configurar o controlo da actividade das aplicações

Para editar uma regra de monitorização de actividade perigosa, seleccione-a a partir da lista e especifique as definições da regra na parte inferior do separador:

- Especifique a reacção da Defesa pró-activa em relação à actividade perigosa.

Pode especificar uma das seguintes acções como reacção: permitir, perguntar o que fazer e bloquear. Clique com o botão esquerdo do rato na ligação da acção até que a mesma assuma o valor que necessita. Para além de parar o processo, você pode colocar em Quarentena a aplicação que iniciou a actividade perigosa. Para o fazer, utilize a ligação On / Off a partir da definição adequada. Pode atribuir um intervalo de tempo para a frequência com que se executará a verificação para detectar processos ocultos no sistema.

- Especifique se é necessário gerar um relatório sobre a operação executada. Para o fazer, utilize a ligação On. / Off.

Para desligar a monitorização para uma actividade perigosa, desmarque a caixa ☑ que aparece junto ao nome das actividades perigosas na lista.

Especificidades da configuração do controlo da actividade das aplicações no Kaspersky Anti-Virus com o Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou Microsoft Windows Vista x64:

Se possui um dos sistemas operativos acima listados, só é controlado um tipo de eventos de sistema, *comportamento perigoso*. O Kaspersky Anti-Virus para Windows Workstations analisa a actividade das aplicações instaladas no seu computador e detecta actividades perigosas ou suspeitas, com base na lista de regras criadas pelos especialistas da Kaspersky Lab.

Se pretende que o Kaspersky Anti-virus monitorize a actividade dos processos do sistema, para além dos processos de utilizadores, seleccione a caixa **Vigiar contas de utilizadores do sistema** (ver Figura 34). Por defeito, esta opção está desactivada.

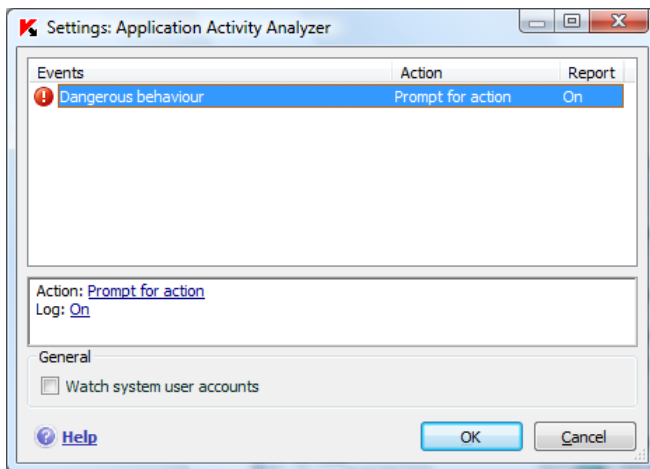



Figura 34. Configurar o controlo da integridade das aplicações no Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista, Microsoft Windows Vista x64

As contas de utilizadores controlam o acesso ao sistema e identificam o utilizador no seu ambiente de trabalho, o que impede que outros utilizadores corrompam o sistema operativo ou os dados. Os processos do sistema são processos iniciados por contas de utilizadores do sistema.

10.1.2. Monitorização de Macros VBA

Esta componente da Defesa Pró-activa não funciona com o Microsoft Windows XP Professional Edição x64, Microsoft Windows Vista ou Microsoft Windows Vista x64.

Pode activar a verificação e processamento das macros perigosas executadas no seu computador, assinalando a caixa ☑ **Activar a Monitorização de Macros VBA**. Cada macro executada é analisada e se estiver na lista de macros perigosas, esta é processada.

Exemplo:

> A macro *PDFMaker* é um plug-in do Adobe Acrobat que existe na barra de ferramentas do Microsoft Office Word e que permite criar um ficheiro .pdf a partir de qualquer documento. A Defesa pró-activa classifica como perigosas certas acções, como sejam a incorporação de elementos em programas. Se a monitorização de macros VBA estiver activada, quando for carregada uma macro, a Defesa pró-activa exibirá um aviso no ecrã,

informando-o que foi detectado um comando de macro perigoso. Você pode escolher terminar aquela macro ou permiti-la.

Pode configurar quais as acções a aplicar quando forem executadas macros com acções suspeitas. Se tiver a certeza de que essa macro não é perigosa ao trabalhar com um determinado ficheiro, por exemplo, um documento do Microsoft Word, recomendamos que crie uma regra de exclusão. Se ocorrer uma situação que corresponde aos termos da regra de exclusão, a acção suspeita executada pela macro não será processada pela Defesa pró-activa.

Para configurar verificações de macros:

1. Abra a janela de definições do Kaspersky Anti-Virus para Windows Workstations, clicando em Definições na janela principal do programa.
2. Seleccione a **Defesa pró-activa** na árvore de definições.
3. Clique no botão **Definições** na secção **Activar Monitorização de Macros VBA**.

As regras de processamento de macros perigosas são configuradas na janela **Definições da Monitorização de Macros VBA** (ver Figura 35) Esta janela contém regras predefinidas para comportamentos que a Kaspersky Labs classifica como sendo perigosos. As acções para macros perigosas incluem, por exemplo, módulos que incorporam em programas e apagam ficheiros.

Se não considera perigoso um determinado comportamento da lista, desmarque a caixa que aparece junto ao nome do mesmo. Por exemplo, você pode usar frequentemente macros para abrir ficheiros (que não têm o atributo de "apenas leitura") e tem a certeza que esta operação não é maliciosa.

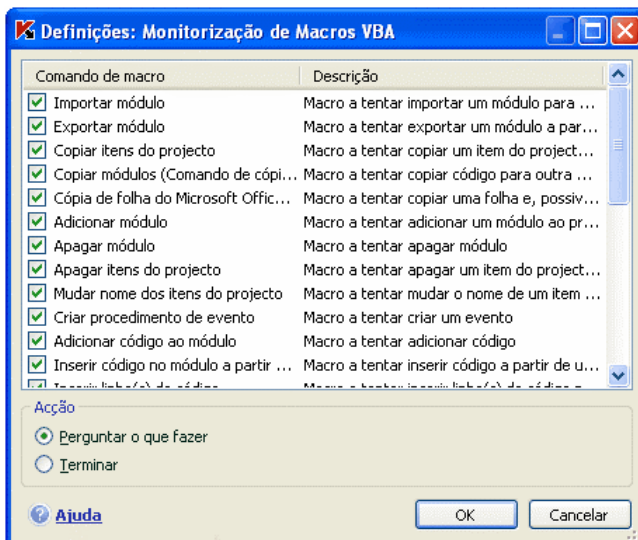



Figura 35. Configurar opções da Monitorização de Macros

Para que o Kaspersky Anti-virus para Windows Workstations não bloqueie a macro:

desmarque a caixa que aparece antes dessa acção. O programa deixará de considerar aquela macro como perigosa e a defesa pró-activa não a processará.

Por defeito, sempre que o programa detectar uma acção iniciada por uma macro no seu computador, a aplicação perguntar-lhe-á se deseja permitir ou bloquear essa macro.

De forma a que o programa bloqueie, automaticamente, todo o comportamento perigoso sem perguntar primeiro ao utilizador:

Na janela com a lista de macros seleccione **Terminar**.

10.1.3. Monitorização do registo

O objectivo de muitos programas maliciosos é o de editar o registo do sistema operativo do seu computador. Estes programas podem ser programas de brincadeiras inofensivos (joke programs) ou outros programas maliciosos que representam uma ameaça real para o seu computador.

Por exemplo, os programas de brincadeiras conseguem copiar as suas informações para a chave de registo que faz com que as aplicações sejam automaticamente abertas com a inicialização do sistema.

Para configurar a monitorização do registo do sistema:

1. Abra a janela de opções do Kaspersky Anti-virus para Windows Workstations clicando em Definições na janela principal do programa.
2. Seleccione a Defesa Pró-activa na árvore de definições.
3. Clique no botão **Definições** na secção **Activar Monitorização do Registo**.

Os especialistas da Kaspersky Lab já criaram uma lista de regras que controlam as operações com chaves de registo e incluíram-na no programa. As operações com chaves de registo desagregam-se em grupos lógicos tais como *Segurança do Sistema, Segurança da Internet*, etc. Cada um desses grupos inclui chaves de registo do sistema e regras para trabalhar com as mesmas. Quando você actualiza o programa, são adicionados a esta lista novos grupos de regras para chaves.

A janela **Definições**: **Monitorização do Registo** (ver Figura 36) apresenta uma lista completa das regras.

Cada grupo de regras tem uma prioridade de execução que pode aumentar ou reduzir, utilizando os botões **Mover cima** e **Mover baixo**. Quanto mais alto estiver o grupo na lista, mais elevada é a prioridade atribuída ao mesmo. Se um mesmo ficheiro de registo estiver em diversos grupos, a primeira regra a ser aplicada àquele ficheiro será a regra do grupo com a prioridade mais elevada.

Pode parar de utilizar qualquer grupo de regras da seguinte forma:

- Desmarque a caixa ☑ que aparece antes do nome do grupo. Neste caso, o grupo de regras permanecerá na lista, mas a Defesa pró-activa não o utilizará.
- Apague o grupo de regras da lista. Recomendamos que não apague os grupos criados pelos especialistas da Kaspersky Lab, visto que esses grupos contém o conjunto de regras mais adequadas.

Você pode criar os seus próprios grupos de objectos do registo do sistema monitorizados. Para o fazer, clique em **Adicionar** na janela de grupos de objectos.

Siga estes passos na janela que se abre:

1. Insira o nome do novo grupo para a monitorização das chaves de registo do sistema, no campo **Nome** do grupo.
2. Seleccione o separador **Chaves** e crie uma lista de ficheiros de registo que serão incluídas no grupo monitorizado (ver 10.1.3.1 na pág. 139)

para o qual pretende criar as regras. Isso pode envolver uma ou várias chaves.

3. Seleccione o separador **Regras** e crie uma regra para ficheiros (ver 10.1.3.2 na pág. 140) que se aplicará às chaves seleccionadas no separador Chaves. Pode criar várias regras e estabelecer a ordem pela qual são aplicadas.

Figura 36. Grupos de chaves de registo controlados

10.1.3.1. Seleccionar chaves de registo para criar uma regra

O grupo de objectos criado deve conter, pelo menos, um ficheiro de registo do sistema. O Separador **Chaves** fornece uma lista de ficheiros aos quais a(s) regra(s) se aplicam.

Para adicionar um ficheiro de registo do sistema:

1. Clique no botão **Adicionar** na janela **Editar…** (ver Figura 37).
2. Na janela que se abre, seleccione o ficheiro de registo ou uma pasta de ficheiros, para os quais pretende criar a regra de monitorização.
3. Especifique o valor da chave ou uma máscara para um grupo de objectos, ao qual pretende aplicar a regra, no campo **Valor**.
4. Seleccione a opção ☑ **Incluir subchaves** para que a regra se aplique a todas os ficheiros anexados ao ficheiro de registo listado.

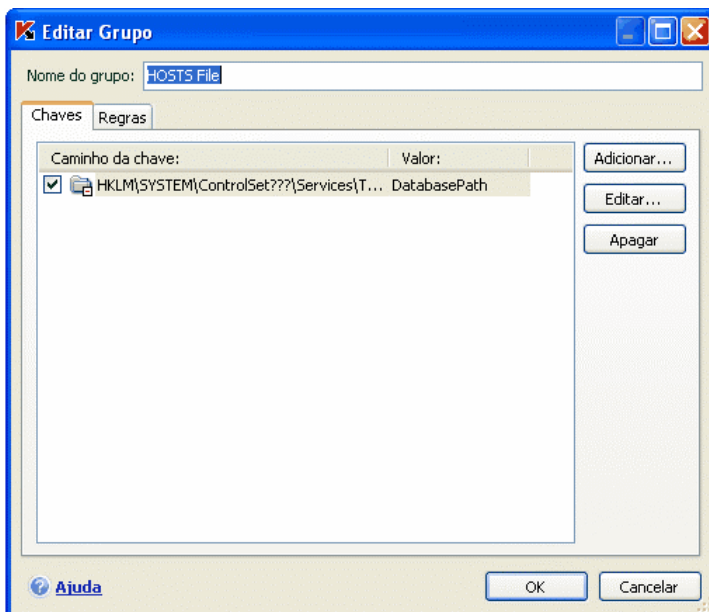



Figura 37. Adicionar chaves de registo controladas

O uso em simultâneo da máscara com um asterisco ou ponto de interrogação e da opção assinalada ☑ **Incluir subchaves** apenas é necessário se esses símbolos forem utilizados no nome da chave.

Se seleccionar um grupo de chaves no registo, utilizando uma máscara, e especificar um valor específico para o mesmo, a regra será aplicada àquele valor para qualquer chave do grupo seleccionado.

10.1.3.2. Criar uma regra de Monitorização de Registo

Uma regra de Monitorização do Registo especifica:

- O programa cujo acesso ao registo do sistema está a ser monitorizado
- A reacção da Defesa pró-activa quando um programa tenta executar uma operação com um ficheiro do registo do sistema

Para criar uma regra para os ficheiros do registo do sistema que seleccionou:

1. Clique em **Nova** no Separador **Regras**. A nova regra será adicionada como a primeira da lista de regras (ver Figura 38).
2. Seleccione uma regra na lista e especifique as definições da regra na parte inferior do separador:
   - Especifique a aplicação.

     Por defeito, a regra é criada para qualquer aplicação. Se pretender que a regra seja aplicada a uma aplicação em específico, clique com o botão esquerdo do rato na ligação Qualquer aplicação e esta mudará para Esta aplicação. Depois use a ligação Especificar o nome da aplicação. Abrir-se-á um menu de contexto e, se clicar em **Procurar**, você pode ir para a janela padrão de selecção de ficheiro ou, se clicar em **Aplicações**, você pode ir para uma lista das aplicações actualmente em funcionamento e seleccionar as que necessitar.
   - Defina a reacção da Defesa pró-activa, em relação à tentativa da aplicação seleccionada para ler, editar ou apagar chaves de registo do sistema.

     Pode usar qualquer uma das seguintes acções como reacção: permitir, perguntar o que fazer e bloquear. Clique com o botão esquerdo do rato na ligação da acção até que a mesma assuma o valor que necessita.
   - Especifique se é necessário gerar um relatório sobre a operação executada. Para o fazer, clique em log / não gerar log.

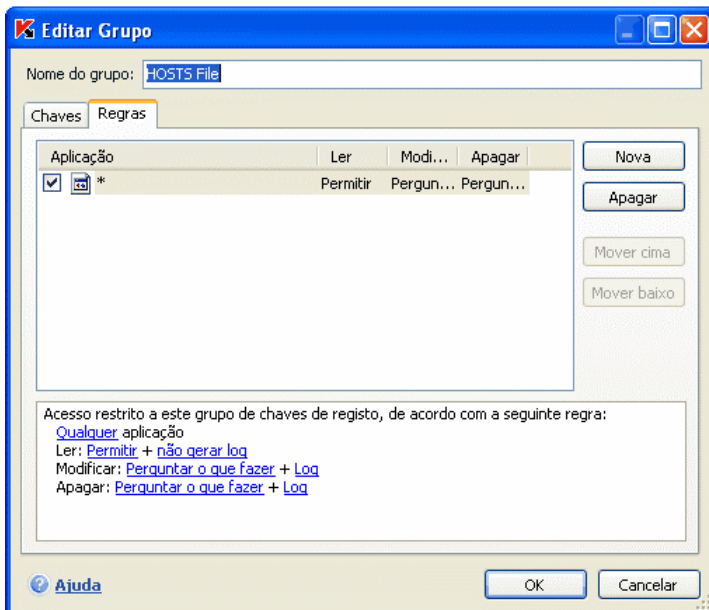



Figura 38. Criar uma regra de monitorização da chave de registo

Pode criar várias regras e ordená-las segundo a sua prioridade, utilizando os botões **Mover Cima** e **Mover Baixo**. Quanto mais alta estiver a regra na lista, mais elevada é a prioridade atribuída à mesma.

Também pode criar uma regra de *permissão* (ou seja, todas as acções são permitidas) para um objecto de registo do sistema, a partir da janela de notificação que informa que um programa está a tentar executar uma operação com um objecto. Para o fazer, clique em Criar regra de permissão na notificação e, na janela que se abre, especifique o objecto de registo do sistema ao qual a regra será aplicada.

CAPÍTULO 11. ANTI-SPY

A componente do Kaspersky Anti-Virus para Windows Workstations que o protege em relação a todos os tipos de software malicioso é o *Anti-Spy*. Recentemente, o malware (software malicioso) tem vindo a incluir mais e mais programas que têm como objectivo:

- Roubar os seus dados confidenciais, incluindo passwords, números do cartão de crédito, documentos importantes, etc.
- Registar as suas acções no computador e analisar o software instalado no mesmo.
- Entregar, de forma intrusiva, conteúdos publicitários em navegadores da Internet, janelas de pop-up e faixas de publicidade (banners) em diversos programas.
- Obter acesso não autorizado à Internet, a partir do seu computador para aceder a diversos sites.

Os ataques de phishing e interceptores de teclado concentram-se em roubar as suas informações; os autodialers (ligações telefónicas automáticas), programas de brincadeiras (joke programs) e adware (software com publicidade) podem consumir o seu tempo e o seu dinheiro. O Anti-Spy foi concebido para proteger o seu computador em relação a estes programas.

O Anti-Spy inclui os seguintes módulos:

- O *Anti-Phishing* protege-o de ataques de phishing.

  Em termos gerais, o phishing consiste em e-mails enviados a partir de supostas instituições financeiras que contêm links para os seus sites. A mensagem de texto convence o leitor a clicar no link e a inserir informações confidenciais na janela que se abre em seguida, como por exemplo, um número de cartão de crédito ou um nome de utilizador e password para um site de Internet banking.

  Um exemplo comum de phishing é um e-mail de um banco que você utiliza com um link para o site oficial desse banco. Ao clicar nesse link, você é direccionado para uma cópia exacta do site do banco, onde até pode ver o endereço verdadeiro do banco no navegador, apesar de, na verdade, estar num site falsificado. A partir deste momento, todas as acções que executar no site são registadas e podem ser utilizadas para roubar o seu dinheiro.

  Você pode receber um link para um site de phishing site através de um e-mail ou por outros meios, como por exemplo uma mensagem do ICQ. O Anti-Phishing regista as tentativas para abrir sites de phishing e bloqueia essas tentativas.

As assinaturas de ameaças do Kaspersky Anti-Virus para Windows Workstations incluem todos os sites que são actualmente conhecidos como sendo usados para phishing. Os especialistas da Kaspersky Lab reabastecem-no com endereços obtidos através do Anti-Phishing Working Group, uma organização internacional. Você preenche esta lista ao actualizar as assinaturas de ameaças.

- O *Bloqueador de Popups* bloqueia as janelas de popup que contêm anúncios com links para diversos sites.

  A informação contida nestas janelas, normalmente, não é benéfica. Estas janelas abrem-se, automaticamente, quando você abre um determinado site ou acede a uma outra janela utilizando uma hiperligação. Estas contêm anúncios publicitários e outras informações que você não solicitou sob qualquer forma. O Bloqueador de Popups bloqueia estas janelas e surge uma mensagem especial por cima do ícone da bandeja do sistema que o informa acerca disso. Você pode decidir, directamente a partir desta mensagem, se pretende bloquear ou não a janela.

  > O Bloqueador de Popups funciona adequadamente com o módulo de bloqueio de pop-up do Microsoft Internet Explorer incluído no Service Pack 2 do Microsoft Windows XP. Quando instala o Kaspersky Anti-Virus para Windows Workstations, é instalado um plugin no navegador que lhe permite dar autorização a janelas de pop-up para que se abram directamente no seu navegador da Internet.

  Alguns sites usam as janelas de pop-up para lhe disponibilizar informação de forma mais fácil e rápida. Se você usa, frequentemente, esse tipo de sites e se a informação contida nas janelas de pop-up é extremamente importante para si, você pode adicioná-los à lista de sites confiáveis. (ver 11.1.1 na pág. 145) de forma a que as suas janelas de popup não sejam boqueadas.

  Ao utilizar o Microsoft Internet Explorer, o ícone aparecerá na barra de estado do navegador quando uma janela de popup for bloqueada. Pode desbloqueá-la ou adicionar o endereço à lista de endereços confiáveis, clicando sobre o mesmo.

- O *Anti-Banner* bloqueia anúncios contidos em banners especiais na Internet ou incorporados nas interfaces de programas instalados no seu computador.

  As faixas de publicidade não só são desprovidas de informação útil, como também o distraem do seu trabalho e aumentam o volume de tráfego no seu computador. O Anti-Banner bloqueia as faixas de publicidade mais comuns, com base nas máscaras criadas pelo Kaspersky Anti-Virus para Windows Workstations. Você pode desactivar

o bloqueio de faixas de publicidade ou criar as suas próprias listas de banners permitidos ou bloqueados.

> Para integrar o Anti-Banner no programa **Opera**, adicione a seguinte linha ao ficheiro *standard_menu.ini*, secção **[Image Link Popup Menu]**:
>
> Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 para Windows Workstations\opera_banner_deny.vbs", "//nologo %C"

- O *Anti-Dialer* protege-o em relação a ligações não autorizadas através do seu modem.

> O Anti-Dialer funciona no Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista e Microsoft Windows Vista x64.

Os dialers, normalmente, estabelecem ligações a sites específicos, tais como sites com material pornográfico. Depois você é forçado a pagar tráfego de Internet dispendioso, que você nunca desejou ou utilizou. Se desejar excluir um determinado número da lista bloqueada, deve colocá-lo na lista de números confiáveis (ver 11.1.3 na pág. 150).

11.1. Configurar o Anti-Spy

O Anti-Spy protege-o de todos os programas conhecidos pelos especialistas da Kaspersky Lab que possam roubar as suas informações confidenciais ou o seu dinheiro. Você pode configurar a componente de forma mais específica:

- Criando uma lista de sites confiáveis (ver 11.1.1 na pág. 145) cujas janelas de popup não deseja bloquear
- Criando listas “negras” e listas “brancas” de banners (ver 11.1.2 na pág. 147)
- Criando listas de números de telefone confiáveis (ver 11.1.3 na pág. 150) para as ligações de acesso telefónico que você permite

11.1.1. Criar uma lista de endereços confiáveis no Bloqueador de Popups

Por defeito, o Bloqueador de Popups bloqueia todas as janelas de pop-up que aparecem automaticamente sem que você as abra. A excepção são as janelas

de sites adicionados à lista de sites confiáveis do Microsoft Internet Explorer e os sites de Intranet, nos quais você está registado naquele momento.

Se você estiver a utilizar o Windows XP com o Service Pack 2, o Internet Explorer já tem o seu próprio bloqueador de pop-up. Você pode configurá-lo, seleccionando, em particular, quais as janelas que deseja bloquear e quais as que deseja permitir. O Bloqueador de Popups permite trabalhar com este bloqueador de acordo com o seguinte princípio: quando uma janela de pop-up tenta abrir-se, uma regra de bloqueio terá sempre a prioridade. Por exemplo, o endereço de uma determinada janela de pop-up está na lista de janelas permitidas para o Internet Explorer, mas não para o Bloqueador de Popups. Esta janela será bloqueada. Por esta razão, se estiver a utilizar o Microsoft Windows XP Service Pack 2, recomendamos que configure, em conjunto, o navegador de Internet e o Bloqueador de Popups.

Se pretender visualizar qualquer janela, por uma ou outra razão, deve adicioná-la à lista de endereços confiáveis. Para o fazer:

1. Abra a janela de Definições do Kaspersky Anti-Virus para Windows Workstations e seleccione o **Anti-Spy** na árvore de definições.
2. Clique em **Sites Confiáveis** na secção **Activar Bloqueador de Popups**.
3. Clique em **Adicionar** na janela que se abre (ver Figura 39) e insira uma máscara para os sites cujas janelas de pop-up você não pretende bloquear.

> Dica:
>
> Ao inserir uma máscara de endereço confiável, você pode usar os caracteres * ou ?. Por exemplo, a máscara http://www.test* exclui os pop-ups de qualquer site que comece com aquela série de caracteres.

4. Especifique se os endereços, incluídos na zona confiável do Internet Explorer ou nos endereços na sua rede de área local, serão excluídos da verificação. Por defeito, o programa considera-os confiáveis e não bloqueia as janelas de pop-up destes endereços.

A nova exclusão será adicionada ao início da lista de endereços confiáveis. Para parar de utilizar a exclusão que você adicionou, basta desmarcar a caixa ☑ que surge antes do respectivo nome. Se você desejar remover, por completo, uma exclusão, seleccione-a na lista e clique em **Apagar**.

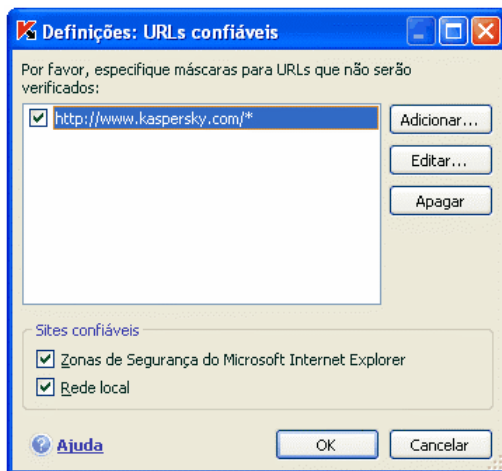



Figura 39. Criar uma lista de endereços confiáveis

Se você pretender bloquear pop-ups da sua Intranet (Rede Local) ou sites incluídos na lista de sites confiáveis do Microsoft Internet Explorer, desmarque as respectivas caixas na secção **Sites confiáveis**.

Quando as janelas de pop-up, que não estão incluídas na lista endereços confiáveis, se tentarem abrir, surgirá uma mensagem sobre o ícone do programa que informa que a janela foi bloqueada. Através das ligações que surgem nessa mensagem, você pode cancelar o bloqueio e adicionar o endereço da janela à lista de endereços confiáveis.

Você pode adoptar acções semelhantes, trabalhando com o Internet Explorer tal como vem incluído no Windows XP Service Pack 2. Para o fazer, utilize o menu de contexto, que você pode abrir sobre o ícone do programa na parte inferior do navegador de Internet, quando as janelas de pop-up estão bloqueadas.

11.1.2. Lista de bloqueio de faixas de publicidade

O *Anti-Banner* é componente do Kaspersky Anti-Virus para Windows Workstations responsável por bloquear faixas de publicidade. Os especialistas da Kaspersky Lab compilaram uma lista de máscaras dos banners mais comuns, com base em pesquisas especialmente desenvolvidas, e incluíram-na no programa. Se o Anti-Banner não estiver desactivado, este bloqueia os banners que estiverem seleccionados através das máscaras nesta lista.

Você também pode criar uma lista branca e uma lista negra de faixas de publicidade, as quais irão permitir ou bloquear banners.

> Note que se você tiver uma máscara de domínio na lista para banners bloqueados ou numa lista negra, você ainda conseguirá aceder ao site raiz.
>
> Por exemplo, se a lista de banners bloqueados incluir uma máscara para **truehits.net**, você conseguirá aceder ao URL **http://truehits.net**, mas o acesso ao URL h**ttp://truehits.net/a.jpg** será bloqueado.

11.1.2.1. Configurar a lista de bloqueio de banners comuns

O Kaspersky Anti-Virus para Windows Workstations inclui máscaras para os banners mais comuns incluídos em sites e interfaces de programas. Esta lista é compilada pelos especialistas da Kaspersky Lab e é actualizada juntamente com as assinaturas de ameaças.

Você pode seleccionar que máscaras de banners comuns deseja usar quando utilizar o Anti-Banner. Para o fazer:

1. Abra a janela das Definições do Kaspersky Anti-Virus para Windows Workstations e seleccione o Anti-Spy na árvore de definições.
2. Clique no botão **Definições** na secção Anti-Banner.
3. Abra o Separador **Geral** (ver Figura 40). O Anti-Banner bloqueará as máscaras de banners listadas no separador. Você pode utilizar metacaracteres em qualquer parte do endereço do banner.

A lista de máscaras comuns bloqueadas não pode ser editada. Se não deseja bloquear um banner abrangido por uma máscara comum, desmarque a caixa ☑ que surge antes da máscara.

Para analisar faixas publicitárias (banners) que não correspondem às mascaras da lista padrão, assinale a opção ☑ **Usar métodos de análise heurística**. Depois a aplicação analisará as imagens carregadas em termos de sinais típicos de banners. Depois desta análise, a imagem pode ser identificada como um banner e bloqueada.

Você também pode criar as suas próprias listas de banners permitidos e bloqueados. Pode fazê-lo nos Separadores **Lista Branca** e **Lista Negra**.

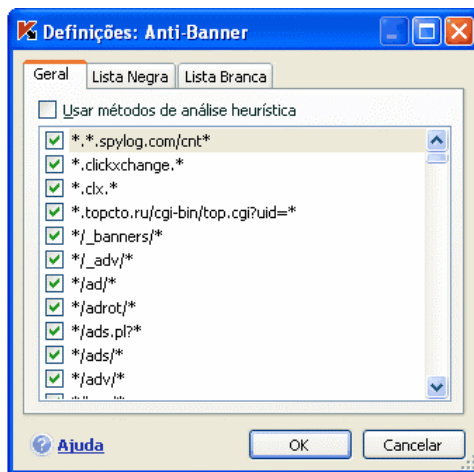



Figura 40. Lista de banner bloqueados

11.1.2.2. Listas brancas de banners

Os utilizadores criam listas brancas de banners, enquanto utilizam o programa, se não precisarem de bloquear determinados banners. Esta lista contém máscaras para banners permitidos.

Para adicionar uma máscara nova à *lista branca:*

1. Abra a janela das Definições do Kaspersky Anti-Virus para Windows Workstations e seleccione o Anti-Spy na árvore de definições.
2. Clique no botão **Definições** na secção **Anti-Banner**.
3. Abra o Separador **Lista Branca**.

Adicione a máscara de banner permitida através do botão **Adicionar**. Você pode especificar o URL completo para o banner ou uma máscara para o mesmo. Neste último caso, quando um banner tenta executar-se, o programa irá verificar o seu endereço por comparação com a máscara especificada.

Ao criar uma máscara, pode usar metacaracteres * ou **?** (onde * representa uma sequência de caracteres e ? – qualquer caractere único).

Para deixar de utilizar uma máscara que criou, você não tem que apagá-la da lista; basta desmarcar a caixa que surge antes da mesma. Desse modo, os banners que se incluem nesta máscara não serão processados como uma exclusão.

Ao utilizar os botões **Importar** e **Exportar**, você pode copiar as listas de banners permitidos que criou de um computador para outro.

11.1.2.3. Listas negras de banners

Para além da lista de banners comuns bloqueados (ver 11.1.2.1 na pág. 148) pelo Anti-Banner, você pode criar a sua própria lista. Para o fazer:

1. Abra a janela das Definições do Kaspersky Anti-Virus para Windows Workstations e seleccione o Anti-Spy na árvore de definições.
2. Clique no botão **Definições** na secção **Anti-Banner**.
3. Abra o Separador **Lista Negra**.

Utilize o botão **Adicionar** e insira uma máscara para o banner que você deseja que o Anti-Banner bloqueie. Você pode especificar o URL completo para o banner ou uma máscara para o mesmo. Neste último caso, quando um banner tenta executar-se, o programa irá verificar o seu endereço por comparação com a máscara especificada.

> Ao criar uma máscara, pode usar metacaracteres ***** ou **?** (onde * representa uma sequência de caracteres e ? – qualquer caractere único).

Para deixar de utilizar uma máscara que criou, você não tem que apagá-la da lista; basta desmarcar a caixa ☑ que surge antes da mesma.

Utilizando os botões **Importar** e **Exportar**, pode copiar de um computador para o outro as listas dos banners bloqueados que criou.

11.1.3. Criar uma lista de números confiáveis no Anti-Dialer

A componente *Anti-Dialer* monitoriza números de telefone utilizados para fazer ligações secretas à Internet. Uma ligação é considerada secreta se estiver configurada para não informar o utilizador sobre a ligação ou se for uma ligação que você não inicia por sua própria iniciativa.

Sempre que ocorre uma tentativa de ligação secreta, o programa notifica-o, exibindo uma mensagem especial no ecrã. Nessa janela de aviso, você tem que decidir se deseja permitir ou bloquear essa ligação. Se você não tiver iniciado esta ligação, é muito provável que se deva a um programa malicioso.

Se deseja permitir ligações a determinados números, sem que o programa lhe pergunte o que fazer, deve adicioná-los à lista de números confiáveis. Para o fazer:

1. Abra a janela das Definições do Kaspersky Anti-Virus para Windows Workstations e seleccione o Anti-Spy na árvore de definições.
2. Clique em **Números confiáveis** na secção Anti-dialer.
3. Clique em **Adicionar** na janela que se abre (ver Figura 41) e insira um número ou uma máscara para os números de telefone confiáveis.

> Dica:
>
> Quando inserir uma máscara de número confiável, você pode utilizar os caracteres * ou ?.
>
> Por exemplo, 0???? *79787* irá abranger quaisquer números que comecem com 79787 para os quais o código da área inclua 4 dígitos.*

O novo número de telefone será adicionado ao início da lista de números confiáveis. Para parar de utilizar a exclusão do número que adicionou, basta desmarcar a caixa ☑ que surge antes do mesmo. Se deseja remover completamente uma exclusão, seleccione-a na lista e clique em **Apagar**.

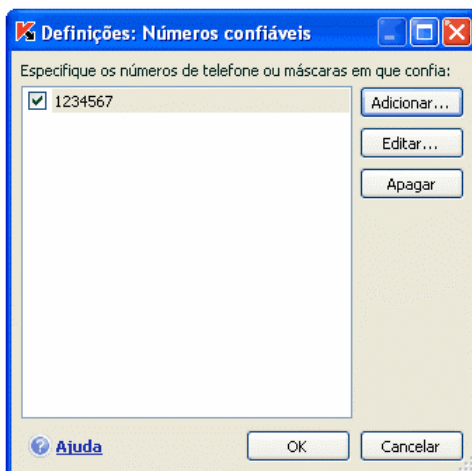
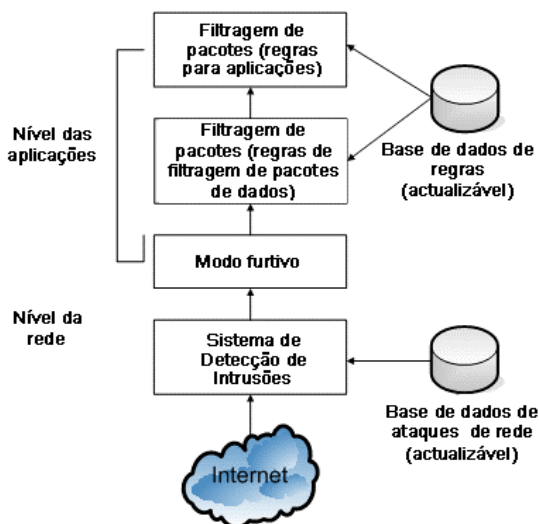



Figura 41. Criar uma lista de endereços confiáveis

CAPÍTULO 12. PROTECÇÃO EM RELAÇÃO A ATAQUES DE REDE

Hoje em dia, os computadores ficam muito vulneráveis quando estão ligados à Internet. Eles estão sujeitos tanto a infecções de vírus como a outros tipos de ataques que se aproveitam da vulnerabilidade dos sistemas operativos e do software.

O Kaspersky Anti-Virus para Windows Workstations contém um componente, o Anti-Hacker, para assegurar a sua segurança nas redes locais e na Internet. Ele protege o seu computador ao nível da rede e das aplicações e mascara o seu computador na Internet de maneira a prevenir ataques. Vejamos melhor como é que o Anti-Hacker funciona.

Você está protegido ao <u>nível da rede</u> ao utilizar regras globais de filtragem de pacotes onde a actividade da rede for permitida ou bloqueada, com base em definições de análise tais como a direcção dos pacotes, o protocolo de transferência de dados e a porta dos pacotes a enviar. As regras para pacotes de dados definem o acesso à rede, independentemente das aplicações instaladas no seu computador que utilizam a rede.

Além das regras de filtragem de pacotes, o *Sistema de Detecção de Intrusões* (SDI) fornece segurança adicional ao nível da rede. O objectivo do sistema é o

de analisar as ligações de entrada, detectar pesquisas de portas no seu computador e filtrar pacotes de rede destinados a explorar as vulnerabilidades do software. Durante o funcionamento, o Sistema de Detecção de Intrusões bloqueia todas as ligações de entrada a partir de um computador atacante durante um certo período de tempo e o utilizador recebe uma mensagem a dizer que o seu computador sofreu um ataque de rede.

O Sistema de Detecção de Intrusões baseia-se na utilização de uma base de dados de ataques de rede (ver 12.9 na pág. 171) em análise, que é alargada regularmente pela Kaspersky Lab e é actualizada juntamente com as assinaturas de ameaças.

O seu computador está protegido ao nível das aplicações ao aplicar regras de aplicações para a utilização dos recursos da rede nas aplicações instaladas no seu computador. Tal como o nível da segurança da rede, o nível da segurança das aplicações baseia-se na análise de bases de dados para direcções, protocolos de transferência e as portas que eles utilizam. No entanto, ao nível das aplicações, são tomadas em consideração tanto as características do pacote de dados, como a aplicação específica que envia e recebe o pacote.

A utilização das regras de aplicações ajuda-o a configurar uma protecção mais específica quando, por exemplo, um certo tipo de ligação é banido nalgumas aplicações mas noutras não.

Existem dois tipos de regras Anti-Hacker, com base nos níveis de segurança Anti-Hacker:

- *Regras de filtragem de pacotes* (ver 12.3 na pág. 160). Utilizadas para criar restrições gerais na actividade de rede, independentemente das aplicações instaladas. Exemplo: se criar uma regra de filtragem de pacotes que bloqueia as ligações de entrada na porta 21, nenhuma das aplicações que utiliza essa porta (um servidor ftp, por exemplo) poderá ser acedida a partir do exterior.
- *Regras de aplicações* (ver 12.2 na pág. 155). Utilizadas para criar restrições na actividade da rede para aplicações específicas. Exemplo: se tem regras de bloqueio para ligações na porta 80 para todas as aplicações, pode criar uma regra que permita ligações naquela porta apenas para o Firefox.

Existem dois tipos de regras de aplicações e de filtragem de pacotes: *permitir* e *bloquear*. A instalação do programa inclui um conjunto de regras que regulam a actividade da rede para as aplicações mais comuns e utilizando os protocolos e portas mais comuns. O Kaspersky Anti-Virus para Windows Workstations também inclui um conjunto de regras para aplicações confiáveis cuja actividade não gera suspeitas.

O Kaspersky Anti-Virus para Windows Workstations divide todo o espaço da rede em *zonas* para tornar as definições e regras mais fáceis de utilizar: *Internet*

e *zonas de segurança*, que correspondem largamente às sub-redes a que o seu computador pertence. Pode atribuir um estado a cada zona (*Internet, Rede Local, Confiável*), que determina a política para aplicação de regras e monitorização da actividade da rede naquela zona (ver 12.5 na pág. 165).

Uma funcionalidade especial do Anti-Hacker, o *Modo Furtivo*, impede o computador de ser detectado a partir do exterior, de forma a que os hackers não consigam detectar o computador para o atacar. Este modo não afecta o desempenho do seu computador na Internet: recomenda-se que não utilize o Modo Furtivo se o seu computador estiver a funcionar como servidor.

12.1. Seleccionar um nível de segurança no Anti-Hacker

Quando utiliza a rede, o Kaspersky Anti-Virus para Windows Workstations protege o seu computador num dos seguintes níveis (ver Figura 42):

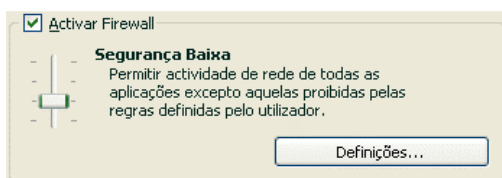



Figura 42. Seleccionar o nível de segurança do Anti-Hacker

Segurança Elevada – a actividade de rede é permitida conforme estipulado pela regra de permissão. O Anti-Hacker utiliza as regras que vieram com o programa ou que você criou. O conjunto de regras incluídas no Kaspersky Anti-Virus para Windows Workstations inclui regras de permissão para aplicações cuja actividade da rede não é suspeita e para pacotes de dados que são absolutamente seguros para enviar e receber. No entanto, se na lista de regras existir uma regra de bloqueio para uma aplicação com prioridade mais elevada do que a regra de permissão, o programa bloqueará a actividade de rede para essa aplicação.

> Aviso!
>
> Se escolher este nível de segurança, será bloqueada qualquer actividade da rede que não esteja definida numa regra de permissão do Anti-Hacker. Por essa razão recomendamos que só utilize este nível se tiver a certeza de que todos os programas de que necessita são permitidos pelas regras e que não planeia instalar software novo.

Modo de Treino – você determina, independentemente, quais as actividades da rede permitidas e bloqueadas. A excepção são as ligações da rede para as quais estão incluídas regras no programa. Neste nível, de cada vez que um programa tentar utilizar um recurso da rede ou transmitir um pacote de dados, o Anti-Hacker verifica se existe uma regra para essa ligação. Se existir uma regra, o Anti-Hacker segue as suas instruções. Se não existir, aparecerá uma mensagem no ecrã. Ela conterá uma descrição da ligação à rede (que programa a iniciou, em que porta, o protocolo, etc.). Você deve decidir se deseja permitir esta ligação ou não. Utilizando um botão especial na janela de mensagem, pode criar uma regra para essa ligação para que, futuramente, o Anti-Hacker utilize as condições na regra para a ligação sem o avisar.

Segurança Baixa – bloqueia a actividade de rede proibida, segundo as regras de bloqueio instaladas pelo programa ou criadas por si. No entanto, se na lista de regras existir uma regra de permissão para uma aplicação com prioridade mais elevada do que a regra de bloqueio, o programa permitirá a actividade da rede para essa aplicação.

Permitir Toda – permite toda a actividade da rede no seu computador. Recomendamos que escolha este nível de protecção em casos extremamente raros quando não tiverem sido observados ataques à rede e você confiar totalmente na actividade da rede.

Pode aumentar ou diminuir o nível de segurança da rede seleccionando o nível que deseja ou alterando as definições do nível actualmente seleccionado.

Para modificar o nível de segurança da rede:

1. Seleccione **Anti-Hacker** na janela de definições do Kaspersky Anti-Virus para Windows Workstations.

2. Ajuste o indicador na secção **Activar Firewall**, para indicar o nível de segurança necessário.

Para configurar o nível de segurança da rede:

1. Seleccione o nível de segurança que melhor se ajusta às suas necessidades.

2. Clique no botão **Definições** e edite as opções de segurança da rede na janela que se abre.

12.2. Regras de aplicações

O Kaspersky Anti-Virus para Windows Workstations inclui um conjunto de regras para as aplicações mais comuns do Windows. Você pode criar várias regras de permissão ou bloqueio para o mesmo programa. Geralmente, estes são

programas com actividade de rede que foi analisada, em detalhe, pelos especialistas da Kaspersky Lab e está estritamente definida como perigosa ou segura.

Dependendo do nível de segurança (ver 12.1 na pág. 154) seleccionado para a Firewall e o tipo de rede (ver 12.5 na pág. 165) em que o computador trabalha, a lista de regras para os programas pode ser utilizada de diversas formas. Por exemplo, no nível **Segurança Elevada** é bloqueada toda a actividade de rede não abrangida pelas regras de permissão.

Para trabalhar com a lista de regras de aplicações:

1. Clique em **Definições** na secção **Activar Firewall** da janela de definições do Anti-Hacker.
2. Na janela que se abre, seleccione o Separador **Regras de Aplicações** (ver Figura 43).

As regras deste Separador podem ser agrupadas através de uma das seguintes formas:

- *Regras por aplicação.* Se estiver seleccionada a opção ☑ **Agrupar as regras por aplicação**, é assim que a lista de regras será exibida. O Separador conterá uma lista de aplicações cujas regras foram criadas. É dada a seguinte informação para cada aplicação: nome e ícone da aplicação, comando de acção, directório de raiz onde está o ficheiro executável da aplicação e o número de regras criadas para a mesma.

  Utilizando o botão **Editar**, pode aceder à lista de regras para a aplicação seleccionada na lista e editá-la: adicionar uma regra nova, editar as regras existentes e alterar a sua posição de prioridade.

  Utilizando o botão **Adicionar,** pode adicionar uma nova aplicação à lista e criar uma regra para a mesma.

  Os botões **Exportar** e **Importar** foram concebidos para transportar as regras criadas para outros computadores. Isto ajuda a configurar rapidamente o Anti-Hacker.

- *Lista geral de regras* sem agrupá-las por aplicação. Pode dispor a lista de regras desta maneira desmarcando a opção ☑ **Agrupar as regras por aplicação**. A lista geral de regras mostra a informação completa sobre uma regra: além do nome da aplicação e do comando para a iniciar, é exibida a acção da regra (permitir ou bloquear a actividade de rede), juntamente com o protocolo de transferência de dados, a direcção dos dados (de entrada ou de saída e outras informações).

  Utilizando o botão **Adicionar**, pode criar novas regras e pode editar uma regra seleccionada na lista através do botão **Editar**. Também poderá editar as definições básicas na parte inferior do Separador.

Pode modificar as prioridades com os botões **Mover cima** e **Mover baixo**.

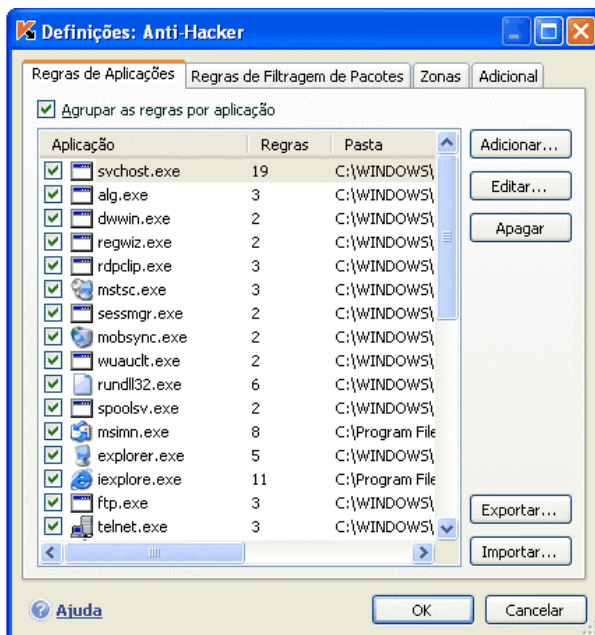



Figura 43. Lista de regras para as aplicações instaladas num computador

12.2.1. Criar regras manualmente

Para criar uma regra de aplicações manualmente:

1. Seleccione uma aplicação. Para o fazer, clique no botão **Adicionar** no Separador **Regras de Aplicações** (ver Figura 43). Isto abrirá um menu de contexto que o levará a uma janela padrão de selecção de ficheiro, através da sua opção **Procurar**, ou para uma lista das aplicações em execução, através da sua opção **Aplicações**, permitindo-lhe fazer a sua selecção. Abrir-se-á uma lista de regras para a aplicação seleccionada. Se já existirem regras para essa aplicação, estas estarão todas listadas na parte superior da janela. Se não existirem regras, a janela de regras estará vazia.

2. Clique no botão **Adicionar** na janela de regra para a aplicação seleccionada.

Pode utilizar a janela **Nova regra** que se abre, para ajustar uma regra (ver 12.6 na pág. 166).

12.2.2. Criar regras a partir de modelos

O Anti-vírus inclui modelos de regras já preparados que poderá utilizar ao criar as suas próprias regras.

A gama completa de aplicações de rede existentes pode ser desagregada em diversos tipos: clientes de e-mail, navegadores de Internet, etc. Cada tipo é caracterizado por um conjunto de actividades específicas, tais como o envio e recepção de e-mails ou a recepção e visualização de páginas html. Cada tipo usa um determinado conjunto de protocolos de rede e portas. É por isso que ter modelos de regras ajuda a fazer as configurações iniciais de regras, rapida e facilmente, com base no tipo de aplicação.

Para criar uma regra de aplicações a partir de um modelo:

1. Seleccione a opção ☑ **Agrupar as regras por aplicação** no separador **Regras de Aplicações**, se ainda não estiver seleccionada, e clique no botão **Adicionar**.

2. Isso apresentará um menu de contexto que o conduzirá a uma janela padrão de selecção de ficheiro através da sua opção **Procurar** ou para uma lista de aplicações em execução através da sua opção **Aplicações**, permitindo-lhe fazer a sua selecção. Abrir-se-á uma lista de regras para a aplicação seleccionada. Se já existirem regras para a mesma, estarão todas listadas na parte superior da janela. Se não existirem regras, a janela de regras estará vazia.

3. Clique em **Modelo** na janela das regras para a aplicação e seleccione um dos modelos de regra a partir do menu de contexto (ver Figura 44).

   Permitir todos é uma regra que permite qualquer actividade de rede para a aplicação. **Bloquear todos** é uma regra que bloqueia qualquer actividade de rede para a aplicação. Todas as tentativas da aplicação em questão, para iniciar uma ligação à rede, serão bloqueadas sem notificar o utilizador.

   Outros modelos listados no menu de contexto criam regras típicas para os programas correspondentes. Por exemplo, o modelo **Cliente de E-Mail** cria um conjunto de regras que permitem as actividades de rede padrão para os clientes de correio, tais como o envio de correio.

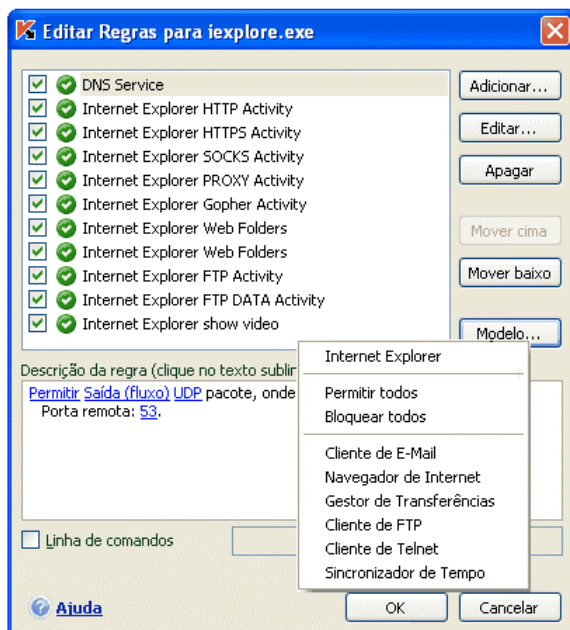



Figura 44. Seleccionar um modelo para criar uma regra nova

4. Se necessário, edite as regras criadas pela aplicação. Pode modificar as acções, a direcção da ligação de rede, endereços remotos, portas (locais e remotas) e o intervalo de tempo para a regra.

5. Se deseja que a regra se aplique a uma aplicação aberta com certas definições na linha de comando, seleccione ☑ **Linha de comandos** e introduza a cadeia no campo à direita.

A regra ou conjunto de regras criadas será adicionada ao final da lista com a prioridade mais baixa. Pode aumentar a prioridade da regra (ver 12.5 na pág. 165).

Pode criar uma regra a partir de uma janela de alerta de detecção da actividade da rede (ver 12.10 na pág. 174).

12.3. Regras de filtragem de pacotes

O pacote de instalação do Kaspersky Anti-Virus inclui um conjunto de regras que o programa utiliza para filtrar os pacotes de dados que entram e saem do computador. Pode iniciar a transferência do pacote de dados ou uma aplicação instalada no seu computador poderá fazê-lo. O programa inclui regras de filtragem de pacotes que os especialistas da Kaspersky Lab analisaram cuidadosamente e definiram como perigosos ou confiáveis.

Dependendo do nível de segurança seleccionado para a Firewall e o tipo de rede em que o computador trabalha, a lista de regras pode ser utilizada de diversas formas. Por exemplo, no nível **Segurança Elevada**, são bloqueados todos os pacotes não abrangidos pelas regras de permissão.

Importante!

Tenha em atenção que as regras de zonas de segurança (ver 12.6 na pág. 166) têm prioridade mais elevada do que as regras de bloqueio de pacotes. Por exemplo, se seleccionar o estado **Rede Local**, o intercâmbio de pacotes será permitido e também o acesso a pastas partilhadas, independentemente das regras de bloqueio de pacotes.

Para trabalhar com a lista de regras de filtragem de pacotes:

1. Clique em **Definições** na secção **Activar Firewall** da janela de definições do Anti-Hacker.
2. Na janela que se abre, seleccione o Separador **Regras de Filtragem de Pacotes** (ver Figura 45).

São fornecidas as seguintes informações para cada regra de filtragem de pacotes: nome da regra, acção (permitir ou bloquear a transferência do pacote), protocolo de transferência de dados, a direcção do pacote e as definições da ligação de rede utilizada para transferir o pacote.

Se o nome para a regra de filtragem de pacotes estiver seleccionado, ele será utilizado.

Você pode trabalhar com a lista de regras utilizando os botões à direita da lista.

Para criar uma nova regra de filtragem de pacotes:

Clique no botão **Adicionar** no Separador **Regras de Filtragem de Pacotes**.

A janela **Nova Regra** que se abre, existe um formulário que poderá utilizar para ajustar uma regra (ver secção 12.4 na pág. 161).

Figura 45. Lista de regras de filtragem de pacotes

12.4. Ajuste de regras para aplicações e filtragem de pacotes

A janela **Nova Regra** para definições avançadas de regras é, praticamente, idêntica para as aplicações e para os pacotes de dados (ver Figura 46).

Primeiro passo:

- Insira um nome para a regra. O programa utiliza um nome padrão que você pode substituir.
- Seleccione as definições de ligação de rede para a regra: endereço IP remoto, porta remota, endereço IP local, intervalo de tempo. Seleccione todas as opções que deseja utilizar na regra.
- Configure outras opções para notificações ao utilizador. Se deseja que apareça uma janela no ecrã com um breve comentário quando uma regra

é utilizada, seleccione ☑ **Exibir aviso**. Se deseja que o programa grave informação sobre o funcionamento da regra no relatório do Anti-Hacker, seleccione a opção ☑ **Log de evento**. A caixa não está seleccionada por predefinição quando é criada a regra. Recomendamos que utilize opções adicionais ao criar regras de bloqueio.

Note que quando cria uma regra de bloqueio no modo de treino do Anti-Hacker, a informação acerca da regra a ser aplicada será, automaticamente, inserida no relatório. Se não precisar de gravar essa informação, desmarque a opção **Log de evento** nas definições para aquela regra.

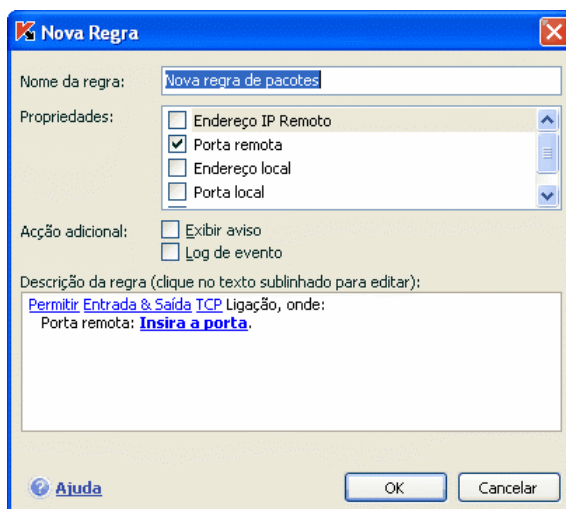



Figura 46. Criar uma nova regra de aplicações

O Segundo passo na criação de uma regra é a atribuição de valores para os parâmetros da regra e a selecção de acções. Estas operações são executadas na secção **Descrição da Regra**.

1. A acção para cada regra criada é *permitir*. Para a transformar numa regra de bloqueio, clique com o botão esquerdo do rato na ligação Permitir na secção de descrição da regra. Esta alterar-se-á para Bloquear.

   O Kaspersky Anti-Virus continuará a analisar o tráfego de rede para os programas e pacotes para os quais foi criada uma regra de permissão. Isso pode fazer com que os dados sejam transmitidos de forma mais lenta.

2. Se antes de criar a regra não seleccionou uma aplicação, precisará de o fazer clicando em Especificar o nome da aplicação. Clique com o botão esquerdo do rato na ligação e, na janela de selecção de ficheiro que se abre, seleccione o ficheiro executável da aplicação para a qual está a criar a regra.

3. Agora precisa de determinar a direcção da ligação à rede para a regra. O valor predefinido é uma regra para ambas as ligações de rede: entrada e saída. Para alterar a direcção, clique com o botão esquerdo do rato em entrada e saída e seleccione a direcção da ligação à rede na janela que se abrir:

   - **Entrada (fluxo)**. A regra é aplicada a ligações de rede abertas por um computador remoto.
   - **Entrada**. A regra aplica-se a pacotes de dados recebidos pelo seu computador, com excepção dos pacotes TCP.
   - **Entrada & Saída**. A regra aplica-se a tráfego de entrada e de saída, independentemente do computador, o seu ou um computador remoto, que iniciou a ligação de rede.
   - **Saída (fluxo)**. A regra apenas é aplicada a ligações de rede abertas pelo seu computador.
   - **Saída**. A regra aplica-se a pacotes de dados transferidos a partir do seu computador, com excepção dos pacotes TCP.

   Se for importante para si definir em específico a direcção dos pacotes na regra, seleccione se são pacotes de entrada ou de saída. Se quiser criar uma regra para um fluxo de dados, seleccione fluxo: saída, entrada ou ambos.

   A diferença entre *direcção do fluxo* e *direcção do pacote* é a seguinte: quando você cria uma regra para um fluxo, você define em que direcção a ligação é aberta. A direcção dos pacotes quando se transferem dados nesta ligação não é tomada em consideração.

   Por exemplo, se configurar uma regra para intercâmbio de dados com um servidor de FTP a funcionar em modo FTP passivo, então tem que permitir um fluxo de entrada. Para o intercâmbio de dados com um servidor de FTP em modo FTP activo, é necessário dar permissão a fluxos de entrada e de saída.

4. Se seleccionou um endereço remoto como uma propriedade para a ligação de rede, então clique com o botão esquerdo do rato sobre a ligação Insira o endereço e, na janela que se abre, insira o endereço IP, intervalo de endereços IP ou endereço de sub-rede para a regra. Para uma mesma regra, pode utilizar um tipo de endereço IP ou vários tipos. Podem ser especificados vários endereços de cada tipo.

5. Depois deverá especificar o protocolo que a ligação de rede utiliza. O protocolo TCP é o protocolo predefinido para a ligação. Se está a criar uma regra para as aplicações, pode seleccionar um de dois protocolos: TCP ou UDP. Para o fazer, clique com o botão esquerdo do rato na ligação com o nome do protocolo, até que ele atinja o valor de que necessita. Se está a criar uma regra para filtragem de pacotes e deseja modificar o protocolo predefinido, clique no nome dele e seleccione o protocolo que precisa na janela que se abre. Se seleccionar ICMP, poderá precisar ainda de indicar o tipo de protocolo.

6. Se seleccionou as definições de ligação de rede (endereço, porta, intervalo de tempo), terá de lhes atribuir valores exactos.

Depois da regra ser adicionada à lista de regras para a aplicação, poderá configurar ainda mais a regra (ver Figura 47). Se desejar aplicá-la a uma aplicação aberta com determinados parâmetros na linha de comando, seleccione a opção **Linha de comandos** e introduza a sequência de parâmetros no campo à direita. Esta regra não se aplicará a aplicações iniciadas com uma chave de acção de comando diferente.

No Microsoft Windows 98, você não dispõe da opção das definições de inicio da linha de comandos.

Pode criar uma regra a partir da janela de alerta de detecção de actividade na rede (ver 12.10 na pág. 174).

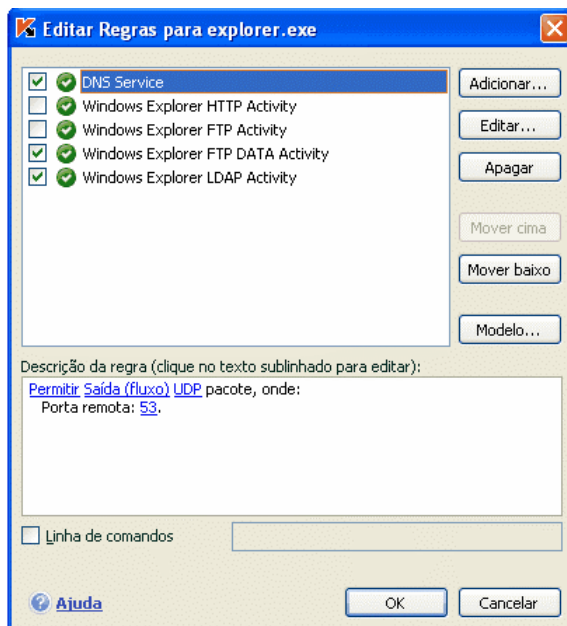



Figura 47. Definições avançadas da nova regra

12.5. Classificação da prioridade da regra

Cada regra de uma aplicação ou pacote tem atribuída uma prioridade de execução. Quando as outras condições são iguais (por exemplo, as definições de ligação à rede), a acção aplicada à actividade do programa será a correspondente à regra que tem a prioridade mais alta.

A prioridade de uma regra depende da sua posição na lista de regras. A primeira regra da lista tem a prioridade mais elevada. Cada regra manualmente criada é adicionada ao início da lista. As regras criadas a partir de modelos ou de notificações são adicionadas ao final da lista de regras.

Para criar prioridades para as regras de aplicação, siga os seguintes passos:

1. Seleccione o nome da aplicação no Separador **Regras de aplicações** e clique no botão **Editar**.

2. Utilize os botões **Mover cima** e **Mover baixo** na janela das regras de aplicações que se abre para mover as regras na lista, modificando desta forma a sua classificação de prioridade.

Para criar prioridades para as regras de filtragem de pacotes, siga os seguintes passos:

1. Seleccione a regra no Separador **Regras de Filtragem de Pacotes**.

2. Utilize os botões **Mover cima** e **Mover baixo** na janela das regras de filtragem de pacotes que se abre para mover as regras na lista, modificando desta forma a sua classificação de prioridade.

12.6. Regras para zonas de segurança

Depois de instalar o Anti-Hacker no seu computador, ele analisará o ambiente de trabalho do seu computador. Com base na análise, ele dividirá todo o espaço de rede em zonas:

Internet – A rede mundial. Nesta zona, o Kaspersky Anti-Virus para Windows Workstations funciona como uma firewall pessoal. Ao fazê-lo, existem regras predefinidas para pacotes e ligações que regulam toda a actividade de rede para garantir o máximo de segurança. Você não pode alterar as definições de protecção quando trabalhar nesta zona, para além de poder activar o Modo Furtivo no seu computador para segurança adicional.

Zonas de segurança – determinadas zonas convencionais que correspondem, sobretudo, a sub-redes nas quais o seu computador está incluído (isso podem ser sub-redes locais em casa ou no trabalho). Por defeito, estas zonas são zonas com um nível de risco médio quando trabalha com elas. Pode alterar os estados destas zonas, com base no seu grau de confiança em relação a uma determinada sub-rede, e pode configurar regras para filtragem de pacotes e para aplicações.

Se o Modo de Treino do Anti-Hacker estiver activado, abrir-se-á uma janela sempre que o seu computador se ligar a uma zona nova, exibindo uma descrição básica sobre ela. Deve atribuir um estado à zona, e a actividade na rede será permitida com base nesse estado. Os valores possíveis para o estado são os seguintes:

- **Internet**. Por defeito, este é o estado atribuído à Internet, visto que quando você acede à Internet, o seu computador está sujeito a todos os tipos de ameaças possíveis. Este estado é também recomendado para redes que não estão protegidas por nenhum programa de anti-

vírus, firewalls, filtros, etc. Quando selecciona este estado, o programa garante segurança máxima enquanto utiliza esta zona, especificamente:

- Bloqueia qualquer actividade de rede NetBios no âmbito da sub-rede.
- Bloqueia regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede:

Mesmo que tenha criado uma pasta partilhada, a informação contida no mesmo não será disponibilizada a utilizadores de sub-redes com este estado. Para além disso, se seleccionar este estado para uma determinada sub-rede, você não poderá aceder a ficheiros e impressoras desta sub-rede.

- **Rede Local**. O programa atribui este estado à maioria das zonas de segurança detectadas na análise do ambiente de rede do seu computador, com excepção da Internet. Recomenda-se que aplique este estado a zonas com um factor de risco médio (por exemplo, Redes de Área Local de empresas). Se seleccionar este estado, o programa dá permissão a:

  - qualquer actividade de rede NetBios no âmbito da sub-rede
  - regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede

  Seleccione este estado se desejar conceder acesso a certas pastas no seu computador, mas bloquear qualquer outra actividade exterior. Os utilizadores, aos quais concede acesso a ficheiros no seu computador, podem utilizar esses ficheiros, mas não podem instalar um Trojan no seu computador.

- **Confiável** – uma rede que sinta que é absolutamente segura e na qual o seu computador não está sujeito a ataques e tentativas para aceder aos seus dados. Quando utiliza este tipo de rede, é permitida toda a actividade de rede. Mesmo se tiver seleccionado a **Protecção Máxima** e tiver criado regras de bloqueio, estas não funcionarão nos computadores remotos de uma rede confiável.

> Note que quaisquer restrições ou acesso a ficheiros só têm efeito sem esta sub-rede.

Poderá utilizar o **Modo Furtivo** para uma segurança acrescida quando utilizar uma rede classificada como **Internet**. Esta funcionalidade apenas permite as actividades de rede que sejam iniciadas por um utilizador ou uma aplicação com permissão para essas actividades. Isto significa que o seu computador se torna

invisível em relação ao que o rodeia. Este modo não afecta a performance do seu computador na Internet.

Não recomendamos o uso do Modo Furtivo se o computador estiver a ser usado como servidor (por exemplo, um servidor de e-mail ou HTTP). Caso contrário, os computadores que se ligam ao servidor não conseguirão vê-lo como estando ligado.

A lista de zonas, nas quais o seu computador está registado, é apresentada no Separador **Zonas** (ver Figura 48). Cada uma das zonas tem atribuído um estado, uma breve descrição da rede e se o Modo Furtivo é utilizado ou não.

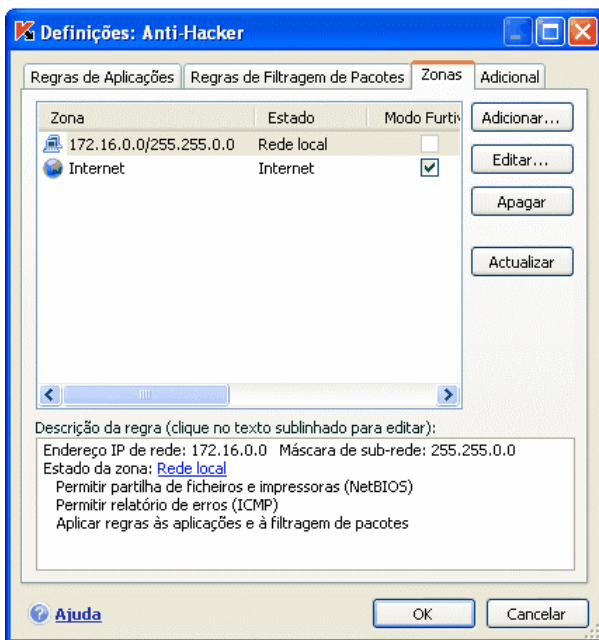



Figura 48. Lista de regras por zonas

Para alterar o estado de uma zona ou para activar/desactivar o **Modo Furtivo**, seleccione-a a partir da lista e utilize as ligações apropriadas na caixa de **Descrição da regra**, que surge por baixo da lista. Pode executar tarefas similares e editar endereços e máscaras de sub-rede na janela **Propriedades da Zona**, janela essa que poderá abrir se clicar em **Editar**.

Pode adicionar uma nova zona à lista enquanto a visualiza. Para o fazer, clique em **Actualizar**. O Anti-Hacker procurará zonas potenciais para registo, e se detectar alguma, o programa pedir-lhe-á para seleccionar um estado para elas.

Além disso, poderá adicionar manualmente novas zonas à lista (se ligar o seu computador portátil a uma nova rede, por exemplo). Para o fazer, utilize o botão **Adicionar** e preencha a informação necessária na janela **Propriedades da Zona**.

Para apagar uma rede da lista, seleccione-a na lista e clique no botão **Apagar**.

12.7. Modo Firewall

O Modo Firewall (ver Figura 49) controla a compatibilidade do Anti-Hacker com os programas que estabelecem ligações de rede múltiplas e com os jogos em rede.

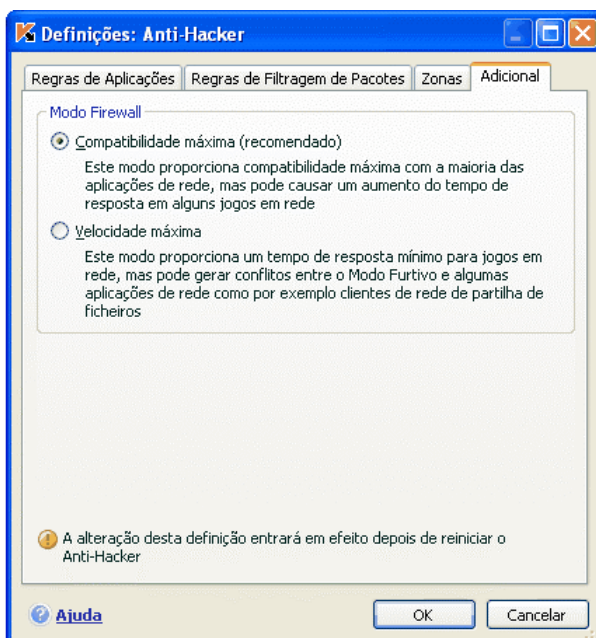



Figura 49. Seleccionar modo Firewall

Compatibilidade máxima – a Firewall assegura que o Anti-Hacker funcionará de forma óptima com os programas que estabelecem ligações de rede múltiplas (clientes de rede de partilha de ficheiros). No entanto, este modo pode levar a um tempo de reacção reduzido nos jogos em rede. Se se deparar com tais problemas, recomenda-se a utilização da Velocidade Máxima.

Velocidade máxima – a Firewall assegura o melhor tempo de resposta possível durante os jogos em rede. No entanto, clientes de rede de partilha de ficheiros ou outras aplicações podem ter conflitos com este modo. Para resolver este problema, desactive o Modo Furtivo.

Para seleccionar um modo Firewall:

1. Abra a janela de definições da aplicação e seleccione a componente **Anti-Hacker** por baixo de **Protecção**.
2. Clique em **Definições** na secção Firewall da janela de definições do Anti-Hacker.
3. Seleccione o Separador **Adicional** na janela que se abre e seleccione o modo que deseja: Compatibilidade máxima ou Velocidade máxima.

> As alterações ao modo Firewall só terão efeito depois do Anti-Hacker ter sido reiniciado.

12.8. Configurar o Sistema de Detecção de Intrusões

Todos os ataques da rede actualmente conhecidos, que poderiam pôr em perigo um computador, estão listados nas assinaturas de ameaças e são actualizador durante a actualização das assinaturas. Por defeito, o Kaspersky Anti-Virus não actualiza as assinaturas de ataques (ver 16.4.2 na pág. 231).

O Sistema de Detecção de Intrusões detecta as actividades de rede típicas dos ataques de rede e se detectar uma tentativa de ataque ao seu computador, bloqueia, durante uma hora, toda a actividade de rede desse computador que envolva o seu computador. Aparecerá um aviso no ecrã dizendo que ocorreu uma tentativa de ataque de rede, com informação específica sobre o computador que o atacou.

Pode configurar o Sistema de Detecção de Intrusões. Para o fazer:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Hacker** por baixo de **Protecção**.
2. Clique em **Definições** na secção **Sistema de Detecção de Intrusões**.
3. Na janela que se abre (ver Figura 50), determine se pretende bloquear um computador atacante e, em caso afirmativo, durante quanto tempo. O tempo predefinido de bloqueio é de 60 minutos. Pode prolongar ou diminuir o tempo de bloqueio, alterando o valor no campo que surge junto à caixa ☑ **Banir o computador atacante durante ... min**. Se

desejar parar de bloquear o tráfego de um computador atacante direccionado ao seu computador, desmarque essa caixa.

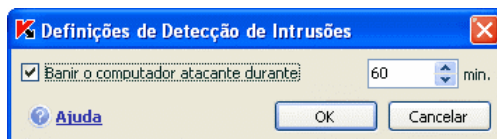



Figura 50. Configurar tempo de bloqueio para computadores atacantes

12.9. Lista de ataques de rede detectados

Hoje em dia existem inúmeros ataques de rede que utilizam as vulnerabilidades dos sistemas operativos e outro software, de sistema ou de outros tipos, instalados no seu computador. Os malfeitores estão constantemente a aperfeiçoar os métodos de ataque, aprendendo como roubar informação confidencial, fazendo com que o seu sistema não funcione ou dominando o seu computador para o utilizar como parte de uma rede zombie para executar outros ataques.

Para assegurar a segurança do seu computador, você precisa de conhecer que tipos de ataques de rede pode encontrar. Os ataques de rede conhecidos podem dividir-se em três grupos:

- **Pesquisa de portas** – esta ameaça não é um ataque, mas habitualmente precede um ataque, já que se trata de uma das formas de obter informação sobre um computador remoto. As portas UDP/TCP utilizadas pelos programas de rede são analisadas para descobrir em que estado estão (fechadas ou abertas).

  As pesquisas de portas indicam ao Hacker que tipos de ataques funcionarão naquele sistema e quais os ataques que não funcionarão. Além disso, a informação obtida pela análise (um modelo do sistema) ajudará o hacker a saber qual o sistema operativo utilizado no computador remoto. Isto, por seu lado, restringirá o número de ataques potenciais, e, correspondentemente, o tempo gasto com eles. Também ajuda um hacker a tentar utilizar as vulnerabilidades particulares desse sistema operativo.

- **Ataques DoS (Recusa de Serviço)** – estes ataques fazem com que o sistema atacado atinja um estado instável ou totalmente inoperável. As consequências destes ataques podem danificar ou corromper os recursos de informação que eles almejam e a impossibilitar o uso desses recursos.

Existem dois tipos básicos de ataques DoS:

- Enviar ao computador alvo pacotes especialmente criados que o computador não espera e que causam o reinício ou a paragem do sistema.
- Enviar ao computador alvo muitos pacotes dentro de um espaço de tempo que o computador não consegue processar, o que esgota os recursos do sistema

Os seguintes ataques são exemplos comuns deste grupo:

- *Ping of Death* consiste no envio de um pacote ICMP superior a 64 KB. Este ataque pode bloquear alguns sistemas operativos.
- *Land* consiste no envio de um pedido para uma porta aberta do seu computador para estabelecer uma ligação com ele próprio. Isto coloca o computador num ciclo, o que intensifica a carga no processador e pode acabar no bloqueio de alguns sistemas operativos.
- *ICMP Flood* consiste no envio de uma larga quantidade de pacotes ICMP para o seu computador. O ataque leva a que o computador seja forçado a responder a cada pacote a receber, o que implica muita carga para o processador.
- *SYN Flood* consiste no envio de uma grande quantidade de consultas para o seu computador para estabelecer uma ligação falsa. O sistema reserva certos recursos para estas ligações, o que esgota completamente os recursos do seu computador, e o computador deixa de reagir a outras tentativas de ligação.

- **Ataques de Intrusão,** que pretendem dominar o seu computador. Este é o tipo de ataque mais perigoso visto que, se for bem sucedido, o hacker terá controlo total sobre o seu computador.

  Os hackers utilizam este ataque quando precisam de obter informação confidencial a partir de um computador remoto (por exemplo, números de cartões de crédito ou passwords) ou de dominar o sistema para utilizar os seus recursos mais tarde com intenções maliciosas (utilizar o sistema capturado em redes zombie ou como plataforma para novos ataques).

  Este grupo também contém mais ataques do que qualquer outro. Podem ser divididos em três subgrupos com base no sistema operativo: ataques Microsoft Windows, ataques Unix e um grupo de serviços de rede que funciona em ambos os sistemas operativos.

  O tipo de ataques mais comum que utiliza as ferramentas de rede do sistema operativo é o seguinte:

- *Ataques de inundação da memória intermédia:* tipo de vulnerabilidade no software que surge devido à falta de controlo ou controlo insuficiente no tratamento de quantidades enormes de dados. Esta é uma das vulnerabilidades mais antigas e a mais fácil para os hackers explorarem.
- *Ataques da cadeia de formato* – tipo de vulnerabilidade no software que surge do controlo insuficiente dos valores de entrada para as funções I/O tais como printf(), fprintf(), scanf(), e outras funções da biblioteca C standard. Se um programa possui esta vulnerabilidade, um hacker, utilizando consultas criadas com uma técnica especial, pode obter o controlo completo do sistema.

O Sistema de Detecção de Intrusões analisa automaticamente e bloqueia tentativas de exploração destas vulnerabilidades nas ferramentas de rede mais comuns (FTP, POP3, IMAP) a funcionar no seu computador.

Os *ataques Microsoft Windows* têm por base o aproveitamento das vulnerabilidades no software instalado no computador (por exemplo, programas como o Microsoft SQL Server, Microsoft Internet Explorer, Messenger e componentes do sistema que podem ser acedidos através da rede – Dcom, SMB, Wins, LSASS, IIS5).

Por exemplo, o Anti-Hacker protege o seu computador de ataques que utilizam as seguintes vulnerabilidades conhecidas (a lista de vulnerabilidades é citada com o sistema de numeração da Microsoft Knowledge Base):

(**MS03-026**) DCOM RPC Vulnerability(Lovesan worm)

(**MS03-043**) Microsoft Messenger Service Buffer Overrun

(**MS03-051**) Microsoft FrontPage 2000 Server Extensions Buffer Overflow

(**MS04-007**) Microsoft Windows ASN.1 Vulnerability

(**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow

(**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling

(**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

Além disso, existem incidentes isolados de ataques de intrusão que utilizam diversos scripts maliciosos, incluindo scripts processados pelo Microsoft Internet Explorer e worms do tipo Helkern. A essência deste tipo de ataques consiste no envio de um tipo especial de pacotes UDP para um computador remoto que poderá executar o código malicioso.

Lembre-se que, enquanto estiver ligado à rede, o seu computador está, constantemente, em risco de ser atacado por um hacker. De forma a assegurar a segurança do seu computador, certifique-se que activou o Anti-Hacker quando utilizar a Internet e actualize regularmente as assinaturas de ataques de hackers (ver 16.4.2 na pág. 231).

12.10. Bloquear e permitir actividade de rede

Se o nível de protecção para a Firewall estiver definido como **Modo de Treino**, cada vez que se tenta estabelecer uma ligação de rede para a qual não existe uma regra, aparece um aviso especial no ecrã.

Por exemplo, depois de abrir o Microsoft Outlook, este transfere os seus e-mails a partir de um servidor remoto de troca. Para apresentar a sua caixa de entrada, o programa liga-se ao servidor de e-mail. O Anti-Hacker examinará sempre este tipo de actividade de rede. Aparecerá uma mensagem no ecrã (ver Figura 51) que contém:

- *Descrição da actividade* – nome da aplicação e um sumário das características da ligação que se está a iniciar. Geralmente, é fornecida informação sobre o tipo de ligação, a porta local a partir da qual a ligação é iniciada, a porta remota e o endereço a que se está a ligar. Para obter informação detalhada sobre a ligação, o processo que a iniciou e sobre o distribuidor da aplicação, clique com o botão esquerdo do rato na área.

- *Acção* – a série de operações que o Anti-Hacker executará em relação à actividade de rede detectada.

Figura 51. Notificação de actividade da rede

Reveja cuidadosamente a informação sobre a actividade de rede e só depois seleccione as acções que o Anti-Hacker executará. Recomendamos que use as seguintes dicas quando tomar uma decisão:

1. Antes de fazer qualquer outra coisa, decida se pretende permitir ou bloquear a actividade de rede. É possível que nesta situação exista um conjunto de regras já criado para esta aplicação ou pacote e que irão ajudá-lo (assumindo que tais regras foram criadas). Para o fazer, use a ligação **Conjunto de Regras**. Nessa altura, será aberta uma janela com uma lista completa das regras criadas para a aplicação ou pacote de dados.
2. Depois decida se pretende executar esta acção uma vez ou automaticamente todas as vezes que esta actividade for detectada.

Para executar a acção só desta vez:

desmarque a opção ☑ **Criar uma regra** e seleccione a acção necessária. Por exemplo, **Permitir**.

Para executar a acção que seleccionou automaticamente sempre que esta actividade for iniciada no seu computador:

1. Seleccione ☑ **Criar uma regra**.
2. Seleccione o tipo de actividade ao qual pretende aplicar essa acção, através da lista suspensa apresentada na secção **Acção**:
   - **Qualquer Actividade** – qualquer actividade de rede iniciada por esta aplicação.

- **Personalizar** – uma actividade individual que terá que definir na janela das regras (ver 12.2.1 na pág. 157).
- **<Modelo>** – nome do modelo que inclui um conjunto de regras típicas da actividade de rede da aplicação. Este tipo de actividade aparece na lista se o Kaspersky Anti-Virus para Windows Workstations possuir um modelo adequado para a aplicação que iniciou a actividade de rede (ver 12.2.2 na pág. 158). Nesse caso, não terá que personalizar que actividades permitir ou bloquear. Use o modelo e será automaticamente criado um conjunto de regras para a aplicação.

3. Clique no botão com o nome da acção (**Permitir** ou **Bloquear**).

Lembre-se que a regra criada apenas será usada quando todos os parâmetros da ligação coincidam com a regra. Por exemplo, esta regra não será aplicada a uma ligação estabelecida a partir de uma porta local diferente.

Para desactivar as mensagens do Anti-Hacker apresentadas para qualquer aplicação que tente estabelecer uma ligação de rede, clique em Desactivar Modo de Treino. Isto colocará o Anti-Hacker no modo Permitir Toda, o qual permite todas as ligações de rede, com excepção daquelas explicitamente proibidas por regras.

CAPÍTULO 13. PROTECÇÃO CONTRA E-MAILS INDESEJADOS

A componente do Kaspersky Anti-Virus para Windows Workstations que detecta spam e o processa de acordo com um conjunto de regras, poupando o seu tempo quando utiliza o correio electrónico, é denominada de *Anti-Spam*.

O Anti-Spam usa o seguinte método para determinar se um e-mail é spam:

1. O endereço do remetente é analisado em relação às correspondências com os endereços das listas negra e branca.

    - Se o endereço do remetente estiver na lista branca, o e-mail é marcado como *Não-Spam*.

    - Se o endereço do remetente estiver na lista negra, o e-mail é marcado como *Spam*. O processamento adicional depende da acção que seleccionou (ver 13.3.7 na pág. 196).

2. Se o endereço do remetente não for encontrado nas listas negra ou branca, o e-mail é analisado usando a tecnologia PDB (ver 13.3.2 na pág. 186).

3. O Anti-Spam examina, em detalhe, o texto do e-mail e procura linhas que façam parte das listas negra ou branca.

    - Se o texto do e-mail contiver linhas que façam parte da lista branca, o e-mail é marcado como *Não-Spam*.

    - Se forem encontradas frases que estão na lista negra de expressões, o e-mail é marcado como *Spam*. O processamento adicional depende da acção que seleccionou.

4. Se o e-mail não contiver frases das listas negra ou branca, o mesmo é analisado em termos de phishing. Se o texto do e-mail contiver um endereço que faz parte da base de dados de phishing, o e-mail é marcado como Spam. O processamento adicional depende da acção que seleccionou.

5. Se o e-mail não contiver linhas de phishing, o mesmo é analisado em termos de spam usando tecnologias especiais:

    - Análise de imagem usando a tecnologia GSG

    - Mensagens de texto analisadas com o algoritmo de reconhecimento de spam: algoritmo de Bayes

6. Por fim, o e-mail é analisado à procura de factores avançados de filtragem de spam (ver 13.3.5 na pág. 193) especificados pelo utilizador quando o Anti-Spam foi instalado. Este processo pode incluir uma análise da exactidão de código HTML, do tamanho de fonte ou de caracteres escondidos.

Você pode desactivar cada um dos passos, acima listados, pelos quais o e-mail passa quando é analisado em termos de spam.

O Anti-Spam está incorporado nos seguintes clientes de e-mail como um plug-in:

- Microsoft Outlook (ver 13.3.8 na pág. 197)
- Microsoft Outlook Express (Programa de E-mail do Windows) (ver 13.3.9 na pág. 200)
- The Bat! (ver 13.3.10 na pág. 202)

Esta versão do Kaspersky Anti-Virus não fornece extensões do Anti-Spam para o Microsoft Office Outlook com o Microsoft Windows 98.

O painel de tarefas para os clientes Microsoft Office Outlook e Microsoft Outlook Express (Programa de E-mail do Windows) tem dois botões, **Spam** e **Não-Spam**, que podem configurar o Anti-Spam para detectar spam dentro da sua caixa de correio. No The Bat! não existem esses botões, contudo o programa pode ser configurado utilizando os itens especiais **Marcar como Spam** e **Marcar como Não-Spam** do menu **Especial**. Para além disso, os parâmetros especiais de processamento de spam (ver 13.3.1 na pág. 185) são adicionados a todas as definições do seu cliente de e-mail.

O Anti-Spam utiliza um algoritmo modificado de iBayes de auto-aprendizagem, que dá mais tempo à componente para melhor distinguir entre *Spam* e *Não-Spam*. O algoritmo extrai dados do conteúdo da mensagem.

Ocorrem situações em que o algoritmo modificado de iBayes é incapaz de classificar, com um grau elevado de exactidão, um determinado e-mail como o Spam ou Não-spam. Estes e-mails são marcados como *Provável Spam*.

De modo a reduzir o número de e-mails que são marcados como *Provável Spam*, recomendamos que efectue um treino adicional do Anti-Spam (ver 13.2 na pág. 180) para tais e-mails. Para o fazer, tem que especificar quais desses e-mails devem ser marcados como *spam* e quais devem ser marcados como *não-spam*.

Os e-mails que são Spam ou Provável Spam são modificados: são adicionadas ao assunto as marcas **[!! SPAM]** ou **[?? Provável Spam]**.

As regras para processar e-mails marcados como spam ou provável spam para o Microsoft Office Outlook, o Microsoft Outlook Express ou The Bat! são definidas em extensões especiais criadas para aqueles clientes de e-mail. Para

outros clientes de e-mail, pode configurar regras de filtragem de modo a terem em conta o assunto e, por exemplo, dependendo se o e-mail contém **[!! SPAM]** ou **[??Provável Spam]** e configurá-las de modo a que movam o e-mail para a pasta correspondente. Para ver mais detalhadamente o mecanismo de filtragem, por favor consulte a documentação do seu cliente de e-mail.

13.1. Seleccionar um nível de sensibilidade do Anti-Spam

O Kaspersky Anti-Virus para Windows Workstations protege-o de spam através de um dos seguintes níveis (ver Figura 52):

Bloquear todas – o nível mais sensível, em que qualquer outro correio à excepção das mensagens que contêm frases da lista branca de expressões (ver 13.3.4.1 na pág. 189) e endereços listados na lista branca de endereços é reconhecido como spam. Neste nível, as mensagens do correio electrónico só são analisadas perante a lista branca. Todas as outras funcionalidades são desactivadas.

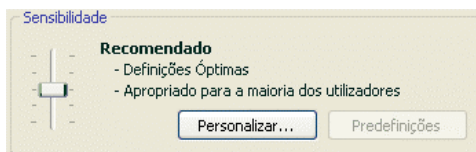



Figura 52. Seleccionar o nível de sensibilidade do Anti-Spam

Elevado – um nível estrito que aumenta a probabilidade de marcar como spam alguns e-mails que não contêm realmente spam. Nessa fase, o e-mail é analisado face às listas negra e branca e também utilizando as tecnologias PDB e GSG e o algoritmo de Bayes (ver 13.3.2 na pág. 186).

Este nível deve ser aplicado nos casos em que há uma probabilidade elevada do endereço do destinatário ser desconhecido dos remetentes de spam. Por exemplo, quando o destinatário não recebe e-mails em massa e não tem o seu endereço de e-mail em servidores de e-mail gratuitos/sem serem empresas.

Recomendado – as definições universais para a classificação de e-mails.

Neste nível, é possível que algum spam não seja detectado. Isto demonstra que o Anti-Spam não está bem treinado. Recomendamos que efectue um treino adicional do módulo, usando o Assistente de Treino (ver 13.2.1 na pág. 181) ou os botões **Spam**/**Não Spam** (ou os itens de menu

correspondentes no The Bat!) para e-mails que foram incorrectamente classificados.

Baixo – o nível de definições mais flexível. Poderá ser recomendado aos utilizadores cuja correspondência a receber, por alguma razão, contém um número significativo de palavras reconhecidas pelo Anti-Spam como spam, mas que na verdade não o são. Isto pode ser por causa da actividade profissional do destinatário, que o força a usar termos profissionais, na sua correspondência com colegas, que são difundidos pelo spam. Neste nível, todas as tecnologias de detecção de spam são utilizadas na análise de correio electrónico.

Permitir todas – o nível menos sensível. Apenas os e-mails que contenham expressões da lista negra e que tenha remetentes listados na lista negra serão reconhecidos como spam. Neste nível, o e-mail só é verificado face à lista negra. Todas as outras definições são desactivadas.

Por defeito, o nível de sensibilidade de protecção de spam está definido em **Recomendado**. Pode elevar ou reduzir o nível ou alterar as definições do nível actualmente seleccionado.

Para modificar um nível de protecção:

Na secção Sensibilidade, ajuste os indicadores para cima ou para baixo para a definição desejada. Ao ajustar o nível de sensibilidade, você define a correlação entre os factores de e-mails spam, provável spam e não-spam (ver 13.3.3 na pág. 187).

Para modificar as definições do nível actualmente seleccionado:

Na janela de definições da aplicação, clique em **Anti-Spam** para apresentar as definições da componente. Clique no botão **Personalizar** na secção Sensibilidade. Na janela que é aberta, edite o factor ou limiar de classificação de spam e clique em **OK**.

O nome do nível de segurança mudará então para **Definições Personalizadas**.

13.2. Treinar o Anti-Spam

O Anti-Spam vem com uma base de dados de e-mails pré-instalada, que contém cinquenta amostras de spam. É recomendado que o módulo Anti-Spam seja submetido a uma configuração adicional através dos seus e-mails.

Há diversas formas de treinar o Anti-Spam:

- Utilizar o Assistente de Treino (ver 13.2.1 na pág. 181)
- Treinar o Anti-Spam com os e-mails de saída (ver 13.2.2 na pág. 182)

- Treinar, directamente, ao trabalhar com e-mails (ver 13.2.3 na pág. 182), utilizando os botões especiais no painel de ferramentas ou os itens de menu dos clientes de e-mail
- Treinar através dos relatórios do Anti-Spam (ver 13.2.4 na pág. 183)

O treino através do Assistente de Treino é o melhor método desde que começa a utilizar o Anti-Spam. O Assistente pode treinar o Anti-Spam num grande número de e-mails.

Note que você não pode treinar o Anti-Spam com mais de 50 e-mails por cada pasta. Se houver mais e-mails numa pasta, o programa apenas usará cinquenta para o treino.

O treino adicional, utilizando os botões especiais na interface do cliente de e-mail é preferível quando trabalha, directamente, com e-mails.

13.2.1. Assistente de Treino

No Assistente de Treino pode treinar o Anti-Spam, indicando quais as pastas de correio que contêm spam e não-spam.

Para abrir o Assistente de Treino:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Clique no botão **Assistente de Treino** na secção Treino da janela de definições.

O Assistente de Treino inclui procedimentos passo a passo para configurar o Anti-Spam. Ao clicar no botão **Seguinte** será levado para a etapa seguinte do treino, e o botão **Anterior** fará com que retroceda à etapa anterior.

A Etapa 1 do Assistente de Treino envolve seleccionar as pastas que contêm os e-mails não-spam. Neste momento, você deve somente seleccionar as pastas cujos conteúdos são de confiança.

A Etapa dois do Assistente de Treino consiste em seleccionar as pastas que contêm spam. Ignore este passo se o seu cliente de e-mail não tiver pastas de spam.

Na Etapa 3, o Anti-Spam é automaticamente treinado nas pastas que seleccionou. Os e-mails daquelas pastas preenchem a base de dados do Anti-Spam. Os remetentes dos e-mails bons são automaticamente adicionados à lista branca de remetentes.

Na Etapa Quatro, os resultados do treino devem ser gravados utilizando um dos seguintes métodos: adicionar os resultados do treino à base de dados actual do Anti-Spam ou substituir a base de dados actual pelos resultados

do treino. Tenha em consideração que o programa deve ser treinado em, pelo menos, 50 e-mails bons e 50 e-mails de lixo electrónico para que a detecção de spam funcione correctamente. Se não o fizer, o algoritmo de iBayes não funcionará.

Para poupar tempo, o Assistente de Treino treina somente 50 e-mails em cada pasta seleccionada.

13.2.2. Treinar com e-mails de saída

Pode treinar o Anti-Spam com e-mails a enviar a partir do seu cliente de e-mail. A lista branca de remetentes do Anti-Spam será preenchida, analisando as mensagens a enviar. Apenas as primeiras cinquenta mensagens de correio electrónico são utilizadas para o treino. Depois disto o treino estará completo.

Para treinar o Anti-Spam com e-mails de saída:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Seleccione ☑ **Treino através de mensagens de e-mail de saída,** na secção **Treino** .

Aviso!

O Anti-Spam só se treinará com e-mails de saída enviados através do protocolo MAPI se seleccionar a opção ☑ **Verificar no momento do envio** no Microsoft Office Outlook, através do plug-in Anti-Vírus de E-mail (ver 13.3.8 na pág. 197).

13.2.3. Treinar através do seu cliente de e-mail

Para treinar enquanto utiliza o seu cliente de e-mail, deve utilizar os botões especiais no painel de ferramentas do seu cliente de e-mail.

Quando instala o Anti-Spam no seu computador, este instala extensões para os seguintes clientes de e-mail:

- Microsoft Outlook
- Outlook Express (Programa de e-mail do Windows)
- The Bat!

Por exemplo, o painel de tarefas do Microsoft Outlook tem dois botões: **Spam** e **Não-Spam** e um separador **Kaspersky Anti-Spam** com definições (ver 13.3.8

na pág. 197) na caixa de diálogo **Opções** (item de menu **Ferramentas→ Opções**). O Microsoft Outlook Express, para além dos botões **Spam** e **Não-Spam**, adiciona um botão de **Configuração** ao painel de tarefas que abre uma janela com acções (ver 13.3.9 na pág. 200) quando é detectado spam. No The Bat! não existem tais botões, embora o programa possa ser treinado utilizando, no menu **Especial**, os itens especiais **Marcar como spam** e **Marcar como NÃO spam**.

Se você decidir que o e-mail seleccionado é spam, clique no botão **Spam**. Se o e-mail não for Spam, clique em **Não-Spam**. Depois disto, o Anti-Spam treinar-se-á com o e-mail seleccionado. Se você seleccionar diversos e-mails, todos os e-mails seleccionados serão utilizados para treino.

Aviso!

Nos casos em que necessita de seleccionar, imediatamente, diversos e-mails ou se estiver certo de que uma determinada pasta apenas contém e-mails de um grupo (spam ou não-spam), pode adoptar uma abordagem abrangente para o treino, utilizando o Assistente de Treino (ver 13.2.1 na pág. 181).

13.2.4. Treinar a partir dos relatórios do Anti-Spam

Você tem a opção de treinar o Anti-Spam a partir dos seus relatórios.

Para ver os relatórios do computador:

1. Na janela principal do programa, na secção **Protecção**, seleccione a componente **Anti-Spam**.
2. Clique com o botão esquerdo do rato na caixa **Estatísticas** (ver Figura 53).

Os relatórios da componente podem ajudá-lo a tirar uma conclusão sobre a exactidão da sua configuração e, se necessário, fazer determinadas correcções ao Anti-Spam.

Para marcar um e-mail como spam ou não-spam:

1. Seleccione-o na lista de relatórios, no Separador **Eventos** e utilize o botão **Acções**.
2. Seleccione uma das quatro opções:
   - **Marcar como “Spam”**
   - **Marcar como Não-Spam**

- **Adicionar à Lista Branca**
- **Adicionar à Lista Negra**

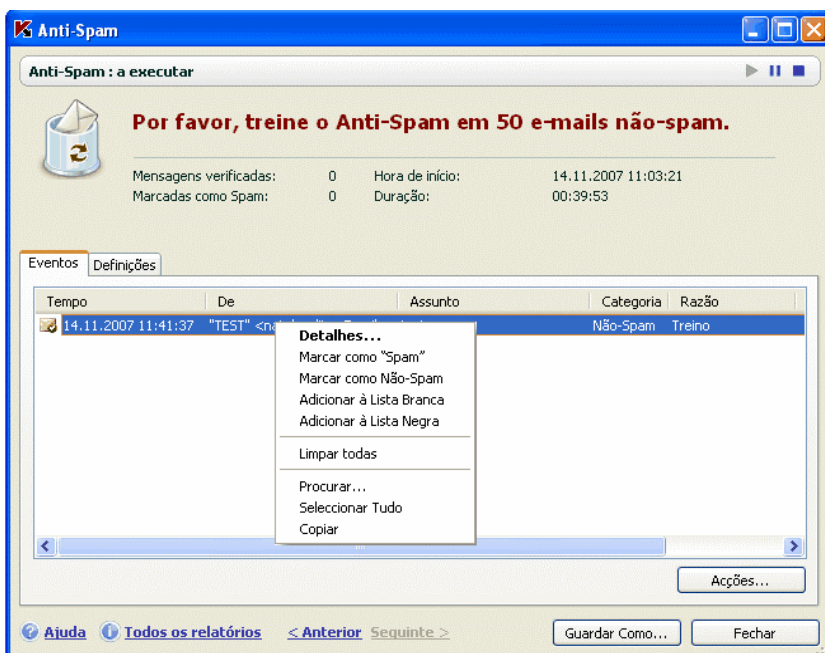



Figura 53. Treinar o Anti-Spam a partir dos relatórios

O Anti-Spam continuará o treino adicional com base nesse e-mail.

13.3. Configurar o Anti-Spam

A configuração do Anti-Spam é essencial para a segurança em relação ao Spam. Todas as definições de funcionamento da componente estão situadas na janela das definições do Kaspersky Anti-Virus para Windows Workstations e permitem-lhe:

- Determinar os detalhes do funcionamento do Anti-Spam (ver 13.3.1 na pág. 185)
- Escolher quais as tecnologias de filtragem de spam a utilizar (ver 13.3.2 na pág. 186)

- Regular a exactidão de reconhecimento de spam e provável spam (ver 13.3.3 na pág. 187)
- Criar as listas branca e negra para remetentes e expressões-chave (ver 13.3.4 na pág. 188)
- Configurar características adicionais de filtragem de spam (ver 13.3.5 na pág. 193)
- Reduzir ao máximo a quantidade de spam na sua caixa de e-mail, através da pré-visualização com o Distribuidor de E-mail (ver 13.3.6 na pág. 195)

As secções que se seguem irão examinar, em detalhe, estas definições.

13.3.1. Configurar definições de análise

Você pode configurar as seguintes definições de análise, para definir se:

- o tráfego dos protocolos de POP3/IMAP deve ser analisado. Por defeito, o Kaspersky Anti-Virus analisa os e-mails em todos estes protocolos.
- as extensões devem ser activadas para o Outlook, Outlook Express (Programa de E-mail do Windows) e o The Bat!.
- os e-mails devem ser visualizados via POP3 no Distribuidor de E-mail (ver 13.3.6 na pág. 195) antes de os transferir do servidor de e-mail para a caixa de correio do utilizador.

Para configurar estas definições:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Assinale ou desmarque as caixas, na secção **Conectividade,** correspondentes às três opções acima discutidas (ver Figura 54).
3. Edite as definições de rede, se necessário.

Figura 54. Configurar opções de análise

Aviso!

Se utiliza o Microsoft Outlook Express deve reiniciá-lo quando alterar o estado da caixa **Activar suporte para o Microsoft Office Outlook, Outlook Express e o The Bat!**.

13.3.2. Seleccionar tecnologias de filtragem de Spam

Os e-mails são analisados quanto à presença de spam, usando tecnologias avançadas de filtragem:

- **iBayes**, baseado no teorema de Bayes, analisa o texto do e-mail para detectar as frases que o marcam como spam. A análise utiliza as estatísticas obtidas no treino do Anti-Spam (ver 13.2 na pág. 180).
- **GSG**, que analisa elementos gráficos nos e-mails, utilizando assinaturas gráficas especiais para detectar spam nos gráficos.
- **PDB**, que analisa os cabeçalhos dos e-mails e os classifica como spam, baseado num conjunto de regras heurísticas.

O programa utiliza, por definição, todas as tecnologias de filtragem, verificando, tão completamente quanto possível, os e-mails para ver se existe spam.

Para desactivar alguma das tecnologias de filtragem:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Na secção **Sensibilidade**, clique em **Personalizar** e, na janela que se abre, seleccione o Separador **Identificação de Spam** (ver Figura 55).
3. Não seleccione as caixas junto às tecnologia de filtragem que não pretende utilizar na detecção de spam.

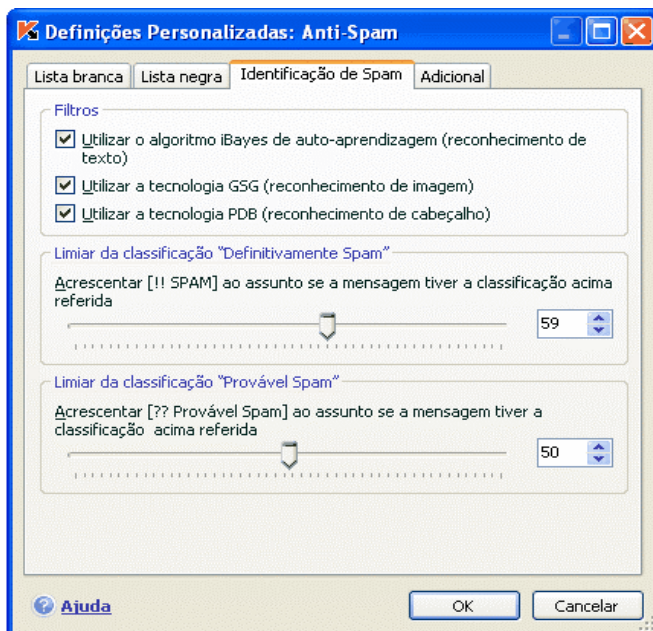



Figura 55. Configurar identificação de spam

13.3.3. Definir as classificações de "Spam" e "Provável Spam"

Os especialistas da Kaspersky Lab configuraram adequadamente o Anti-Spam para reconhecer spam e provável spam.

A detecção de spam funciona com as tecnologias avançadas de filtragem (ver 13.3.2 na pág. 186), treinando o Anti-Spam para reconhecer, com grande exactidão, spam, provável spam e não-spam, através de um determinado número de e-mails da sua caixa de correio.

O Anti-Spam é treinado trabalhando com o Assistente de Treino e a partir dos clientes de e-mail. Assim, durante o treino, a cada elemento individual de e-mail não-spam ou spam é atribuído um factor ou limiar de classificação. Quando um e-mail entra na sua caixa de correio, o Anti-Spam analisa-o com o iBayes, procurando elementos de spam e não-spam. Os factores para cada elemento são totalizados e é atribuído um factor de *spam* e um factor de *não-spam* ao e-mail.

O factor de provável spam define a probabilidade do e-mail ser classificado como provável spam. Se estiver a utilizar o nível **Recomendado**, qualquer e-mail tem a probabilidade entre 50% a 59% de ser considerado *provável spam*. Esse e-mail, depois de ser analisado, tem uma probabilidade inferior a 50 % de ser considerado não-spam. Os e-mails que, depois de ser analisados, tiverem um factor de spam inferior a 50 % serão considerados como não-spam.

O factor de spam determina a probabilidade com que o Anti-Spam classificará um correio electrónico como o spam. Todo o correio electrónico com probabilidades além daquele indicado acima será distinguido como spam. O factor de spam, por definição, é de 59% para o nível **Recomendado**. Isto significa que todo o correio electrónico com uma probabilidade maior do que 59% será marcado como spam.

No total, existem cinco níveis da sensibilidade (ver 13.1 na pág. 179) e, entre esses, três (**Elevado**, **Recomendado** e **Baixo**) baseiam-se em vários valores de factor de spam e provável spam.

Pode alterar o algoritmo do Anti-Spam como pretender. Para o fazer:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Na caixa **Sensibilidade**, do lado direito da janela, clique em **Personalizar**.
3. Na janela que se abre, no Separador **Identificação de Spam**, ajuste os factores de spam e provável spam nas secções correspondentes (ver Figura 55).

13.3.4. Criar manualmente listas brancas e listas negras

Os utilizadores podem criar manualmente listas negras e brancas, utilizando o Anti-Spam com o seu correio electrónico. Estas listas armazenam informação dos endereços de remetentes que são considerados seguros ou spam e as várias palavras-chave e frases que os identificam como spam ou não-spam.

A aplicação principal das listas de frases-chave e, particularmente, da lista branca, é que você pode fazer corresponder com endereços confiáveis, por exemplo, dos seus colegas, assinaturas que contêm uma determinada frase. Pode ser qualquer frase. Pode utilizar, por exemplo, uma assinatura PGP como assinatura. Pode utilizar caracteres especiais nas assinaturas e nos endereços: * e ?. O * representa qualquer sequência de caracteres de qualquer tamanho. Um ponto de interrogação representa qualquer carácter único. Se existirem asteriscos e pontos de interrogação na assinatura, para impedir erros do Anti-Spam ao processá-los, estes devem ser precedidos por uma barra invertida. São então usados dois caracteres em vez de um: * e \?.

13.3.4.1. Listas brancas de endereços e expressões

A lista branca contém frases-chave das mensagens de correio electrónico que você marcou como não-spam e endereços de remetentes que não enviam spam. A lista branca é manualmente preenchida e a lista de endereços de remetentes é criada, automaticamente, durante o treino da componente Anti-Spam. Você pode editar esta lista.

Para configurar a lista branca:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. No lado direito da janela de definições clique em **Personalizar**.
3. Abra o Separador **Lista branca** (ver Figura 56).

O Separador é dividido em duas secções: a zona superior contém os endereços dos remetentes de e-mails não-spam e a parte inferior contém as frases-chave de tais e-mails.

Para activar a lista branca de frases e endereços durante a filtragem de spam, seleccione as caixas correspondentes nas secções **Remetentes Permitidos** e **Expressões Permitidas**.

Você pode editar estas listas, utilizando os botões em cada secção.

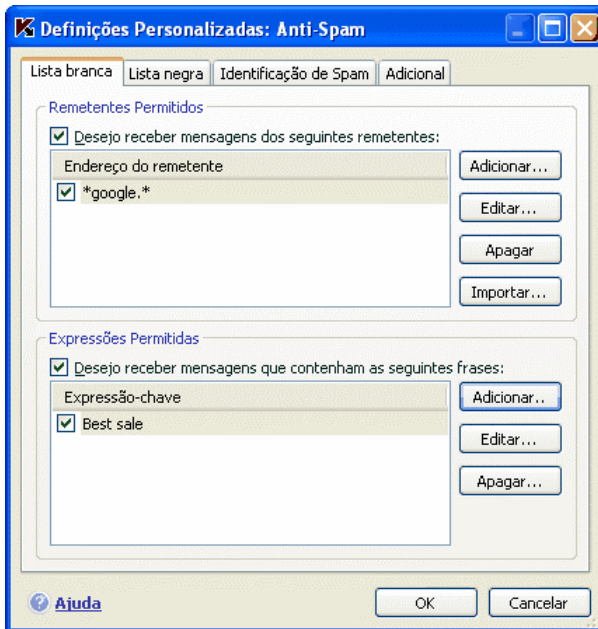



Figura 56. Configurar listas brancas de endereços e frases

Pode adicionar os endereços e máscaras de endereços à lista de endereços. Ao inserir um endereço, o uso de letras maiúsculas é ignorado. Vejamos alguns exemplos de máscaras de endereço:

- *ivanov@test.ru* – as mensagens de correio electrónico deste endereço serão sempre classificadas como não-spam.
- **@test.ru* – as mensagens de correio electrónico de qualquer remetente do domínio test.ru são aceites, por exemplo: petrov@test.ru, sidorov@test.ru;
- *ivanov@** – um remetente com este nome, independentemente do domínio de correio, envia sempre e-mails não-spam, por exemplo: ivanov@test.ru, ivanov@mail.ru;
- **@test** – as mensagens de correio electrónico, de qualquer remetente com um domínio que comece com test, não são spam, por exemplo: ivanov@test.ru, petrov@test.com;
- *ivan.*@test.???* – serão sempre aceites as mensagens de correio electrónico de um remetente cujo nome começa por Ivan. e cujo

domínio começa com o test e acaba com 3 quaisquer caracteres, por exemplo: ivan.ivanov@test.com, ivan.petrov@test.org.

Também pode usar máscaras para frases. Ao inserir uma frase, uso de letras maiúsculas é ignorado. Estão aqui alguns exemplos de algumas:

- *Olá, Ivan!* – uma mensagem de correio electrónico que contenha apenas este texto é aceite. Não se recomenda que utilize uma frase como esta na lista branca de frases.
- *Olá, Ivan!** – uma mensagem de correio electrónico que comece com a frase *Olá, Ivan!* é aceite.
- *Olá, *! ** – as mensagens de correio electrónico que comecem com a saudação *Olá* e um ponto de exclamação em qualquer parte do correio electrónico não são spam.
- ** Ivan? ** – as mensagens de correio electrónico que contenham uma saudação a um utilizador com o nome Ivan, cujo o nome é seguido por um qualquer caracter, não são spam.
- ** Ivan\? ** – as mensagens de correio electrónico que contenham a frase Ivan? são aceites.

Para desactivar o uso de um determinado endereço ou frase como atributos de spam, estes pode ser apagados, utilizando o botão **Apagar,** ou pode desmarcar a caixa junto ao texto para os desactivar.

Você tem a opção de importar ficheiros de formato CSV para a lista branca de endereços.

13.3.4.2. Listas negras de endereços e expressões

A lista negra armazena as frases-chave dos e-mails que são spam e os endereços dos seus remetentes. A lista é preenchida manualmente.

Para preencher a lista negra:

1. Na janela de definições do Kaspersky Anti-Virus para Windows Workstations seleccione o **Anti-Spam**.
2. No lado direito da janela de definições clique em **Personalizar**.
3. Abra o separador **Lista negra** (ver Figura 57).

O Separador é dividido em duas secções: a zona superior contém os endereços de remetentes de spam e a parte inferior contém as frases-chave dessas mensagens de correio electrónico.

Para activar a lista negra de frases e endereços durante a filtragem de spam, seleccione as caixas correspondentes nas secções **Remetentes bloqueados** e **Expressões bloqueadas**.

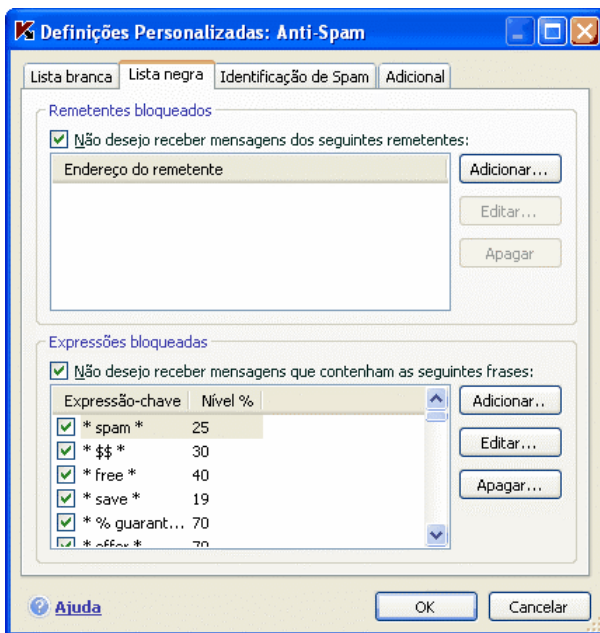



Figura 57. Configurar listas negras de endereços e frases

Pode editar estas listas, utilizando os botões em cada secção.

Pode adicionar endereços e máscaras de endereços à lista de endereços. Ao inserir um endereço, o uso de letras maiúsculas é ignorado. Vamos ver alguns exemplos de máscaras de endereço:

- *ivanov@test.ru* – as mensagens de correio electrónico deste endereço serão sempre classificadas como spam;
- **@test.ru* – as mensagens de correio electrónico de qualquer remetente com o domínio test.ru são spam, por exemplo: *petrov@test.ru, sidorov@test.ru;*
- *ivanov@** – um remetente com este nome, independentemente do domínio de correio, envia apenas spam, por exemplo: *ivanov@test.ru, ivanov@mail.ru;*

- **@test** – as mensagens de correio electrónico, de qualquer remetente com um domínio que comece com test, são spam, por exemplo: *ivanov@test.ru, petrov@test.com;*
- *ivan.*@test.???* – serão sempre spam as mensagens de correio electrónico de um remetente cujo nome começa por ivan. e cujo domínio começa com test e acaba com 3 quaisquer caracteres, por exemplo: *ivan.ivanov@test.com, ivan.petrov@test.org.*

Também pode usar máscaras para frases. Ao inserir uma frase, o registo não é tido em conta. Estão aqui alguns exemplos de algumas:

- *Hi, Ivan!* – uma mensagem de correio electrónico que contenha apenas este texto é spam. Não se recomenda que utilize uma frase como esta na lista negra de frases.
- *Hi, Ivan!** – uma mensagem de correio electrónico que comece com a frase *Hi, Ivan!* é spam.
- *Hi, *! ** – as mensagens de correio electrónico que comecem com a saudação *Hi* e um ponto de exclamação em qualquer parte do e-mail são spam.
- ** Ivan? ** – as mensagens de correio electrónico que contenham uma saudação a um utilizador com o nome *Ivan*, cujo o nome é seguido por um qualquer caracter, são spam.
- ** Ivan\? ** as mensagens de correio electrónico que contenham a frase *Ivan?* são spam.

Para desactivar o uso de um determinado endereço ou frase como atributos de spam, estes pode ser apagados, utilizando o botão **Apagar,** ou pode desmarcar a caixa junto ao texto para os desactivar.

13.3.5. Funcionalidades adicionais da filtragem de spam

Além das funcionalidades principais que são utilizadas para filtrar spam (criar as listas branca e negra, análise de phishing, tecnologias de filtragem), o Kaspersky Anti-Virus para Windows Workstations fornece-lhe funcionalidades avançadas.

Para configurar funcionalidades avançadas de filtragem de spam:

1. Abra a janela de definições da aplicação e seleccione o **Anti-Spam** por baixo de **Protecção**.
2. Na secção **Sensibilidade** da janela de definições, clique no botão **Personalizar**.

3. Abra o separador **Adicional** (ver Figura 58).

O separador regista uma série de indicadores que classificarão o e-mail como sendo, mais provavelmente, spam.

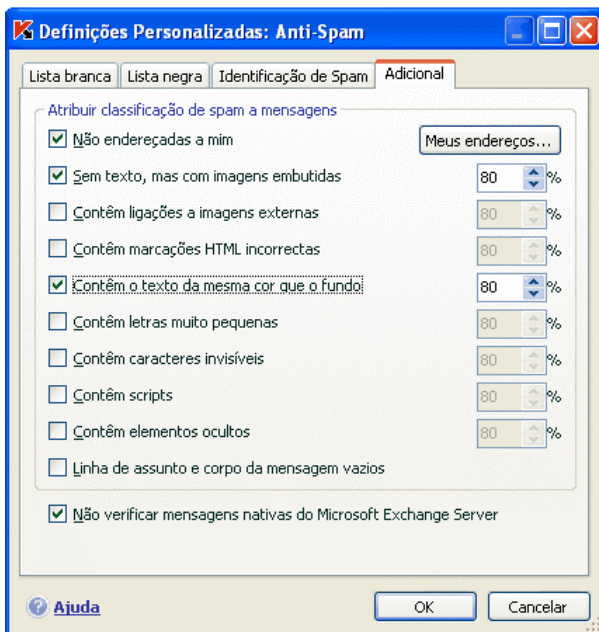



Figura 58. Definições avançadas de reconhecimento de spam

Para usar qualquer indicador de filtragem adicional, seleccione a opção junto ao mesmo. Cada um dos factores requer também que você defina um valor de spam (em percentagem) que define a probabilidade de um e-mail ser classificado como spam. O valor predefinido para o factor de spam é 80%. O e-mail será marcado como spam se a soma das probabilidades de todos os factores adicionais exceder 100%.

O lixo electrónico (Spam) pode ser e-mails vazios (sem assunto ou corpo de texto), e-mails que contenham links para imagens ou com imagens embutidas, o texto da mesma cor que o fundo ou texto em letras muito pequenas. O Spam também pode ser e-mails com caracteres invisíveis (o texto tem a mesma cor que o fundo), e-mails com elementos ocultos (os elementos não são sequer apresentados) ou com marcações HTML incorrectas, assim como e-mails que contenham scripts (uma série de instruções executadas quando o utilizador abre o e-mail).

Se activar a filtragem para as “mensagens não endereçadas a mim”, precisará de criar uma lista de endereços confiáveis acessível através do botão **Meus endereços**. O endereço do destinatário será analisado quando o e-mail for verificado. Se o endereço não corresponder a nenhum dos endereços da sua lista, o e-mail será classificado como *spam*.

Pode criar e editar a lista de endereços na janela **Os Meus Endereços de E-mail**, utilizando os botões **Adicionar**, **Editar** e **Apagar**.

Para excluir da verificação de spam os e-mails reencaminhados dentro da intranet (por exemplo, e-mail empresarial), assinale a opção ☑ **Não verificar mensagens nativas do Microsoft Exchange Server**. Note que os e-mails serão considerados como correio interno se todos os computadores da rede utilizarem o Microsoft Office Outlook como seu cliente de e-mail e se as caixas de correio dos utilizadores estiverem localizadas num servidor de troca ou se estes servidores estiverem conectados com conectores X400. Para que o Anti-Spam analise estes e-mails, desmarque a caixa de selecção.

13.3.6. Distribuidor de E-mail

Aviso!

O Distribuidor de E-mail apenas está disponível se você receber os e-mails através do protocolo POP3.

O Distribuidor de E-mail é criado para ver a lista de e-mails no servidor, sem que o utilizador os tenha que transferir para o seu computador. Deste modo, você pode recusar mensagens, poupar tempo e dinheiro quando trabalha com e-mails e reduzir a probabilidade de transferir spam e vírus para o seu computador.

O Distribuidor de E-mail é aberto se, nas definições do **Anti-Spam**, estiver assinalada a opção ☑ **Exibir Distribuidor de E-mail quando recebe um e-mail**.

Para apagar e-mails do servidor sem os transferir para o seu computador:

> seleccione as caixas à esquerda dos e-mails que devem ser apagados e clique no botão **Apagar.** Os e-mails seleccionados serão apagados do servidor. Os restantes serão transferidos para o seu computador depois de fechar a janela do Distribuidor de E-mail.

Por vezes, pode ser difícil decidir se deve aceitar um determinado e-mail, considerando somente o remetente e o assunto da mensagem. Nesses casos, o Distribuidor de E-mail fornecerá mais informação sobre a mensagem, transferindo o cabeçalho do e-mail.

Para ver os cabeçalhos dos e-mails:

seleccione o e-mail na lista do correio a receber. O cabeçalho do e-mail será apresentado na parte inferior do formulário.

O cabeçalho do e-mail não tem um tamanho significativo, geralmente uma dúzia de bytes e não pode conter código malicioso.

Está aqui um exemplo da utilidade de ver os cabeçalhos. Os remetentes de spam instalaram um programa malicioso no computador de um seu colega de trabalho, que envia spam com o nome nele, usando a lista de contactos do seu cliente de e-mail. A probabilidade de você estar na lista de contactos do seu colega de trabalho é extremamente elevada, o que levará a que a sua caixa de correio seja enchida com esse spam. É impossível julgar, apenas pelo endereço do remetente, se o e-mail foi enviado pelo seu colega de trabalho ou por um remetente de spam. Utilize os cabeçalhos do e-mail! Verifique-os cuidadosamente para saber quem enviou o e-mail, quando e qual o seu tamanho. Siga o trajecto do e-mail desde o remetente até ao seu servidor de correio. Toda esta informação deve estar no cabeçalho do e-mail. Tome uma decisão sobre se é realmente necessário fazer a transferência desse e-mail a partir do servidor ou se o melhor é apagá-lo.

Nota:

Você pode ordenar os e-mails em função de qualquer uma das colunas da lista de e-mails. Para os ordenar, clique no cabeçalho da coluna. As linhas serão ordenadas por ordem ascendente. Para mudar o sentido de ordem, clique de novo no cabeçalho da coluna.

13.3.7. Acções para spam

Se após a análise, você verificar que um e-mail é spam ou provável spam, os próximos passos que o Anti-Spam executa dependem da classificação do ficheiro e da acção seleccionada. Por definição, os e-mails que são spam ou provável spam são alterados: as marcas **[!! SPAM]** ou **[?? Provável spam]** são adicionadas ao assunto.

Pode seleccionar acções adicionais para aplicar a spam ou a provável spam. No Microsoft Outlook, no Microsoft Outlook Express (Programa de E-mail do Windows) e no The Bat! são fornecidas extensões especiais para o fazer. Para os outros clientes de e-mail, pode configurar as regras de filtragem.

13.3.8. Configurar o processamento de spam no Microsoft Office Outlook

> Note que não existem extensões de spam para o Microsoft Outlook se você estiver a utilizar a aplicação com o Windows 9x.

Um e-mail que seja classificado, pelo Anti-Spam, como spam ou provável spam é, por definição, marcado, no **Assunto**, com as marcas especiais: **[!! SPAM]** ou **[?? Provável spam]**.

No Outlook, as acções adicionais para spam e provável spam, podem ser encontradas no separador especial **Anti-Spam**, no menu **Ferramentas** → **Opções** (ver Figura 59).

Este separador é, automaticamente, aberto quando o cliente de e-mail é aberto pela primeira vez, após ter instalado o programa e pergunta se você quer configurar o processamento de spam.

Você pode atribuir as seguintes regras ao processamento para spam e provável spam:

Mover para a pasta – o spam é movido para a pasta da caixa de correio, que você especificar.

Copiar para a pasta – é criada uma cópia do e-mail e é movido para a pasta especificada. O e-mail original mantém-se na sua caixa de correio.

Apagar – apaga o e-mail da caixa de correio do utilizador.

Ignorar – o e-mail fica na caixa de correio electrónico.

Para o fazer, seleccione a opção apropriada na lista pendente na secção de **Spam** ou **Provável spam**.

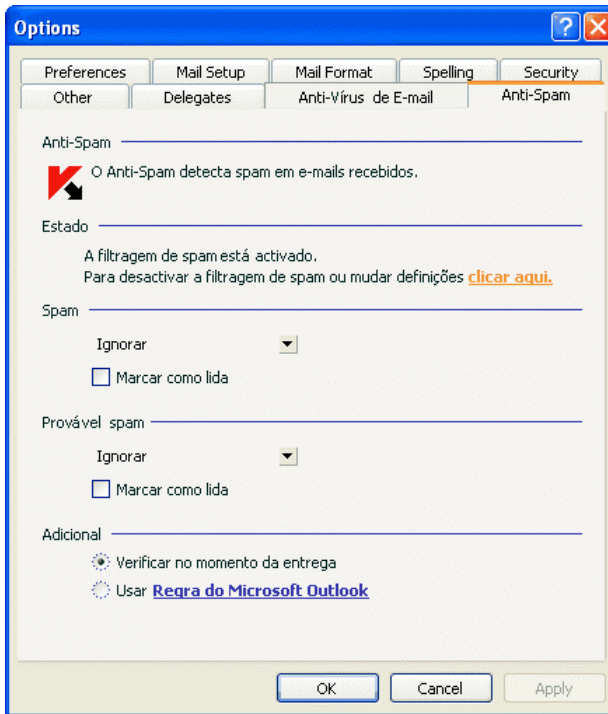



Figura 59. Configurar o processamento de spam no Microsoft Office Outlook

Pode também configurar o Microsoft Office Outlook e o Anti-Spam para trabalharem juntos:

- **Verificar no momento de entrega**. Todos os e-mails que entram na caixa de correio do utilizador são, inicialmente, processados de acordo com as regras do Outlook. Após o processamento estar completo, as extensões do Anti-Spam processam as restantes mensagens que não estão sob a acção de qualquer regra. Por outras palavras, os e-mails são processados de acordo com a prioridade das regras. Por vezes, a ordem das prioridades pode ser ignorada se, por exemplo, chegar um grande número de e-mails ao mesmo tempo à sua caixa de correio. Em tal caso, poderiam acontecer situações em que a informação sobre um e-mail processado por uma regra do Outlook é registada no relatório do Anti-Spam como spam. Para evitar que isto aconteça, recomendamos que configure as extensões do Anti-Spam como uma regra do Outlook.
- **Usar Regra do Microsoft Outlook**. Com esta opção, os e-mails são processados, com base numa hierarquia das regras criadas para o

Microsoft Office Outlook. Uma das regras tem que ser uma regra sobre o processamento de e-mails do Anti-Spam. Esta é a melhor configuração. Não causará conflitos entre o Outlook e as extensões do Anti-Spam. O único inconveniente desta opção é que você deve criar e apagar, manualmente, as regras de processamento de spam do Outlook.

As extensões do Anti-Spam não podem ser utilizadas como uma regra do Outlook no Microsoft Office XP se você estiver a utilizar o 9x/ME/NT4, devido a um erro do Outlook XP.

Para criar uma regra de processamento de spam:

1. Abra o Microsoft Office Outlook e, no menu principal, aceda a **Ferramentas → Regras e Alertas.** O comando para abrir o Assistente depende da versão do Microsoft Office Outlook que está a utilizar. Este Manual de Utilizador descreve como criar uma regra utilizando o Microsoft Office Outlook 2003.

2. Na janela que se abre **Regras e Alertas**, clique em **Nova Regra** no separador **Regras de E-mail** para abrir o Assistente de Regras. O **Assistente de Regras** irá guiá-lo nas seguintes janelas e etapas:

   Etapa Um

   Você pode escolher criar uma regra a partir de um rascunho ou de um modelo. Seleccione **Criar nova regra** e seleccione **Aplique esta regra depois da mensagem chegar**. Clique no botão **Seguinte**.

   Etapa Dois

   Na janela **Condições da Regra**, clique em **Seguinte** sem seleccionar qualquer caixa. Confirme, na caixa de diálogo, que quer aplicar esta regra a todos os mensagens de correio electrónico recebidas.

   Etapa Três

   Na janela para seleccionar acções a aplicar às mensagens, seleccione **Aplicar acção personalizada** na lista de acções. Na zona inferior da janela, clique em acção personalizada. Na janela que é aberta, seleccione **Kaspersky Anti-Spam** no menu suspenso e clique em **OK**.

   Etapa Quatro

   Na janela para seleccionar excepções da regra, clique em **Seguinte** sem seleccionar qualquer caixa.

   Etapa Cinco

   Na janela para terminar a criação da regra, você pode editar o nome da regra (por definição é **Kaspersky Anti-Spam**). Certifique-se que selecciona a opção **Aplicar a regra** e clique em **Concluir**.

3. Por definição, a posição da nova regra é a primeira na lista da janela **Regras de E-mail**. Se preferir, mova esta regra para o fim da lista para que seja aplicada mais tarde aos e-mails.

Todos os e-mails recebidos são processados com estas regra. A ordem com que o programa aplica as regras depende da prioridade que atribuiu a cada regra. As regras começam a ser aplicadas a partir do inicio da lista. Cada regra subsequente está colocada abaixo da anterior. Você pode mudar a prioridade da aplicação das regras aos e-mail.

Se não pretender que a regra do Anti-Spam processe mais e-mails depois de uma regra ser aplicada, você deve seleccionar, nas definições de regras, a opção ☑ **Parar de processar mais regras** (ver Etapa Três em criar uma regra).

Se tiver experiência em criar regras de processamento de e-mail no Outlook, pode criar a sua própria regra para o Anti-Spam baseada nas definições que sugerimos.

13.3.9. Configurar o processamento de spam no Outlook Express (Programa de E-mail do Windows)

Uma mensagem de correio electrónico que seja classificada, pelo Anti-Spam, como spam ou provável spam é, por definição, marcada, no Assunto, com as marcas especiais: **[!! SPAM]** ou **[?? Provável spam]**.

No Outlook Express (Programa de E-mail do Windows), as acções adicionais para spam e provável spam podem ser encontradas na janela de definições que se abre (ver Figura 60) quando clica no botão **Configurações**, que está próximo dos botões do painel de tarefas: **Spam** e **Não-spam**.

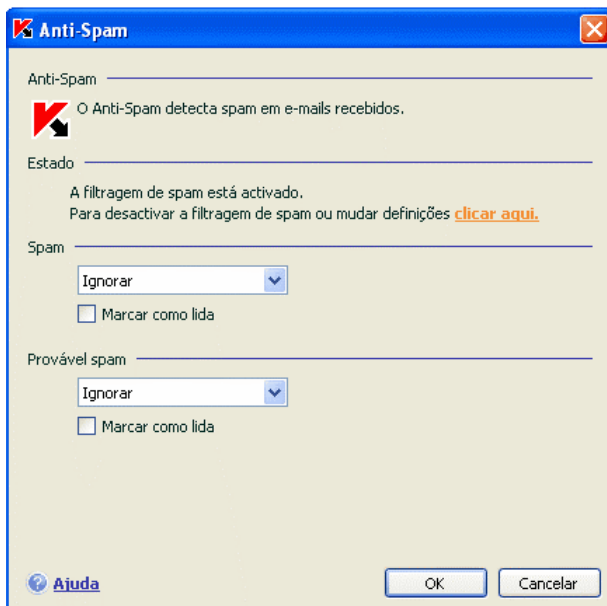



Figura 60. Configurar processamento do spam no Outlook Express

Esta janela abre-se automaticamente quando você inicia pela primeira vez o cliente de e-mail, após ter instalado o programa e pergunta se você quer configurar o processamento de spam.

Você pode atribuir as seguintes regras de processamento para spam e para provável spam:

Mover para pasta – o spam é movido para a pasta da caixa de correio que você especificar.

Copiar para pasta – é criada uma cópia do e-mail e é movido para a pasta especificada. O e-mail original mantém-se na sua caixa de correio.

Apagar – apaga o e-mail da caixa de correio do utilizador.

Ignorar – o e-mail fica na caixa de correio electrónico.

Para o fazer, seleccione a opção apropriada na lista pendente na secção de **Spam** ou **Provável spam**.

13.3.10. Configurar o processamento de spam no The Bat!

O cliente de e-mail deve ser reiniciado depois de activar/desactivar a extensão para o Microsoft Outlook Express.

No The Bat! As acções para spam e para provável spam são definidas pelas próprias ferramentas do cliente.

Para configurar as regras de protecção de e-mail no The Bat!:

1. Seleccione **Definições** no menu **Propriedades**.
2. Na árvore de definições, seleccione **Anti-Spam** (ver Figura 61).

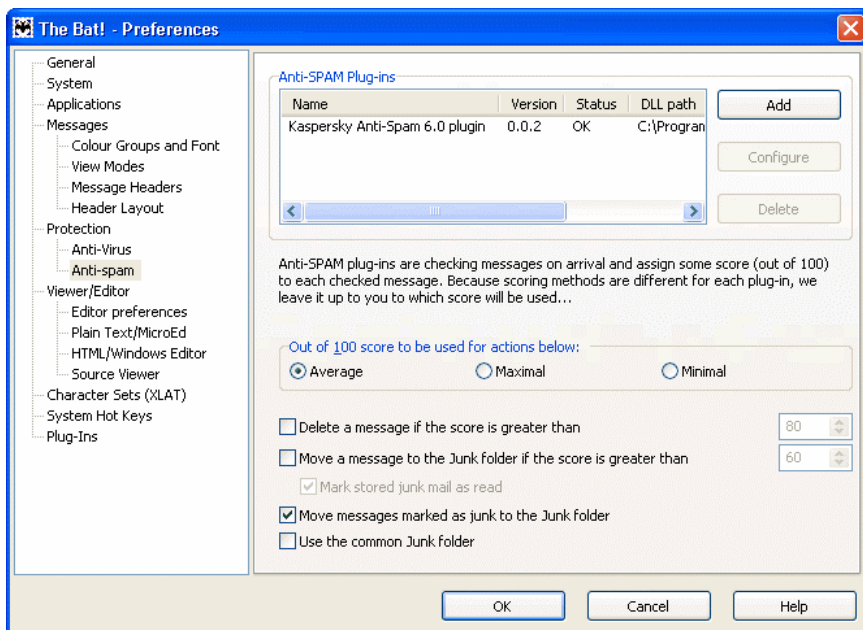



Figura 61. Configurar reconhecimento e processamento do spam no The Bat!

As definições de protecção de spam apresentadas estendem-se a todos os módulos do anti-spam instalados no computador que são compatíveis com o The Bat!.

Você deve ajustar o nível de avaliação e especificar como responder a e-mails com uma determinada avaliação (no caso do Anti-Spam, a probabilidade de que o e-mail é spam):

- Apagar os e-mails com uma avaliação mais elevada do que um dado valor.
- Mover os e-mails com uma dada avaliação para uma pasta especial para spam.
- Mover o spam marcado com os cabeçalhos especiais para a pasta de spam.
- Deixar o spam na sua caixa de correio.

Aviso!

Após ter processado um e-mail, o Kaspersky Anti-Virus para Windows Workstations atribui aos e-mails uma classificação de spam ou provável spam, baseada num factor (ver 13.3.3 na pág. 187) com um valor que pode ajustar. O The Bat! tem o seu próprio método de avaliação de spam, baseado também num factor de spam. Para garantir que não haja alguma discrepância entre o factor de spam do Kaspersky Anti-Virus para Windows Workstations e do The Bat!, a todos os e-mails analisados pelo Anti-Spam é atribuída uma avaliação de acordo as categorias de estado do e-mail utilizadas pelo The Bat!: *correio não-spam* - 0%, *provável spam* - 50%, *spam* - 100%.

Deste modo, a avaliação de spam no The Bat! corresponde não ao factor do e-mail atribuído no Anti-Spam, mas sim ao factor do estado correspondente.

Para mais detalhes sobre a avaliação de spam e regras de processamento, ver a documentação do The Bat!.

CAPÍTULO 14. VERIFICAÇÃO DE VÍRUS NO COMPUTADOR

Um dos aspectos mais importantes na protecção do seu computador contra os vírus é a verificação de vírus em áreas definidas pelo utilizador. O Kaspersky Anti-virus para Windows Workstations pode analisar itens individuais (ficheiros, pastas, discos, mecanismos de Plug & Play) ou o computador inteiro. A verificação de vírus impede a disseminação do código malicioso que passou indetectado nas componentes de protecção.

O Kaspersky Anti-Virus para Windows Workstations inclui as seguintes tarefas de análise predefinidas:

Áreas Críticas

Verifica todas as áreas críticas do computador. Inclui a memória do sistema, programas carregados no arranque, sectores de arranque no disco duro, e os directórios dos sistemas *Windows* e *system32*. A tarefa procura detectar rapidamente vírus activos no sistema sem analisar totalmente o computador.

O Meu Computador

Verifica os vírus no computador com uma inspecção minuciosa de todas as unidades do disco, memória e ficheiros.

Objectos de Inicialização

Verifica todos os programas carregados quando o sistema operativo arranca à procura de vírus.

As definições predefinidas para estas tarefas são as recomendadas. Pode editar estas definições (ver 14.4.4 na pág. 214) ou criar um agendamento (ver 6.5 na pág. 88) para executar tarefas.

Também pode criar as suas próprias tarefas (ver 14.4.3 na pág. 214) e criar um agendamento para as mesmas. Por exemplo, pode criar uma tarefa de verificação para as bases de dados de e-mail uma vez por semana ou uma tarefa de verificação de vírus para qualquer pasta **Os Meus Documentos**.

Além disso, pode analisar qualquer ficheiro em termos de vírus (por exemplo, a unidade rígida onde estão os programas e jogos, bases de dados de e-mails que trouxe para casa do trabalho, um arquivo anexado à mensagem de correio electrónico, etc.) sem ter que criar uma tarefa especial de verificação. Pode seleccionar um ficheiro para analisar a partir da interface do Kaspersky Anti-virus para Windows Workstations ou com as ferramentas normalizadas do sistema operativo do Windows (por exemplo, na janela do programa **Explorador** ou no seu **Ambiente de Trabalho**, etc.).

Pode visualizar uma lista completa de tarefas de análise de vírus para o seu computador, clicando em **Verificar** na parte esquerda da janela principal da aplicação.

14.1. Gerir tarefas de verificação de vírus

Você pode correr uma tarefa de análise de vírus manual ou automaticamente utilizando um agendamento (ver 6.5 na pág. 88).

Para iniciar uma tarefa de análise de vírus manualmente:

Seleccione a caixa junto ao nome da tarefa na secção **Verificar** da janela principal do programa e clique no botão da barra de estado.

As tarefas actualmente em execução são apresentadas (incluindo tarefas criadas através do Kaspersky Administration Kit) são apresentadas no menu de contexto, clicando com o botão direito do rato no ícone de bandeja do sistema.

Para pausar uma tarefa de verificação de vírus:

Clique no botão na barra de estado. O estado da tarefa alterar-se-á para pausado. Isto suspenderá a verificação até que recomece a tarefa novamente de forma manual ou esta recomeçará, automaticamente, de acordo com o agendamento.

Para parar uma tarefa de verificação de vírus:

Clique no botão da barra de estado. O estado da tarefa alterar-se-á para parado. Isto parará a análise até que recomece a tarefa novamente de forma manual ou esta recomeçará, automaticamente, de acordo com o agendamento. A próxima vez que puser a tarefa a funcionar, o programa perguntar-lhe-á se deseja continuar a tarefa onde ela parou ou recomeçar de novo.

14.2. Criar uma lista de objectos a verificar

Para visualizar uma lista de objectos a serem analisados por uma determinada tarefa, seleccione o nome da tarefa (por exemplo, **O Meu Computador**) na secção **Verificar** na janela principal do programa. Será exibida uma lista dos objectos na parte direita do ecrã por baixo da barra de estado (ver Figura 62).

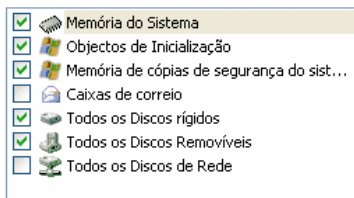



Figura 62. Lista de objectos a analisar

As listas de objectos a analisar estão definidas para as tarefas predefinidas criadas quando instala o programa. Quando você cria as suas tarefas ou selecciona um objecto para uma tarefa de verificação, pode criar uma lista de objectos para essa tarefa.

Você pode adicionar e editar uma lista de verificação de objectos utilizando os botões à direita da lista. Para adicionar um novo objecto de verificação à lista, clique no botão **Adicionar** e, na janela que se abre, seleccione o objecto a ser analisado.

Para conveniência do utilizador, pode adicionar categorias a uma área de verificação, como por exemplo as caixas de e-mail dos utilizadores, a Memória de Acesso Aleatório (RAM), objectos de inicialização, a cópia de segurança do sistema operativo e ficheiros existentes na pasta da Quarentena do Kaspersky Anti-Virus.

Para além disso, quando adiciona uma pasta que contém objectos incorporados a uma área de verificação, você pode editar a recursão. Para o fazer, seleccione um item na lista de verificação, abra o menu de contexto e use a opção **Incluir subpastas**.

Para apagar um objecto, seleccione-o da lista (quando o fizer, o nome do ficheiro será realçado a cinzento) e clique no botão **Apagar**. Pode desactivar temporariamente a verificação de objectos individuais para qualquer tarefa sem os apagar da lista. Para o fazer, desmarque a caixa do objecto que não quer que seja analisado.

Para iniciar uma tarefa de verificação, clique no botão **Verificar** ou seleccione **Iniciar** no menu que se abre quando clicar no botão **Acções**.

Além disso, você também pode seleccionar um ficheiro a ser analisado com as ferramentas standard do sistema operativo Windows (por exemplo, na janela do programa Explorer ou no seu Ambiente de Trabalho, etc.) (ver Figura 63). Para o fazer, coloque o cursor sobre o nome do ficheiro seleccionado, abra o menu de contexto do Windows, clicando com o botão direito do rato, e seleccione **Verificar Vírus**.

Figura 63. Verificar ficheiros a partir do menu de contexto do Windows

14.3. Criar tarefas de verificação de vírus

Para analisar os vírus no servidor, pode utilizar tarefas incorporadas incluídas no programa e criar as suas próprias tarefas. As novas tarefas são criadas com base nas tarefas de verificação que já existem.

Para criar uma tarefa de verificação nova:

1. Seleccione a tarefa com as definições mais próximas das que necessita na secção **Verificar** da janela principal do programa.

2. Abra o menu de contexto clicando com o botão direito do rato ou clique no botão **Acções** à direita da lista de objectos de verificação e seleccione **Guardar como...**

3. Introduza o nome da nova tarefa na janela que se abre e clique em **OK**. Aparecerá uma tarefa com esse nome na lista de tarefas na secção **Verificar** na janela principal do programa.

> Aviso!
>
> Existe um limite no número de tarefas que o utilizador pode criar. Esse limite é de quatro tarefas.

A tarefa criada herda todas as propriedades da tarefa em que se baseou. Você precisa de continuar a configurá-la, criando uma lista de objectos de verificação (ver 14.2 na pág. 205), configurando as propriedades que regularão a tarefa (ver 14.4 na pág. 208) e, se necessário, configurar um agendamento (ver 6.5 na pág. 88) para executar a tarefa automaticamente.

Para renomear a tarefa criada:

Seleccione a tarefa na secção **Verificar** na janela principal do programa, clique com o botão direito do rato para abrir o menu de contexto ou clique no botão **Acções**, na parte direita da lista de objectos de verificação, e seleccione **Alterar Nome**.

Introduza o novo nome da tarefa na janela que se abre e clique em **OK**. O nome da tarefa será então alterado na secção **Verificar**.

Para apagar uma tarefa criada:

Seleccione a tarefa na secção **Verificar** na janela principal do programa, clique com o botão direito do rato para abrir o menu de contexto ou clique no botão **Acções,** na parte direita da lista de objectos de verificação, e seleccione **Apagar**.

Confirme a intenção de apagar a tarefa na janela que lhe pede confirmação. A tarefa será então apagada da lista de tarefas na secção **Verificar**.

Aviso!

Só pode renomear e apagar tarefas que você criou.

14.4. Configurar tarefas de verificação de vírus

Os métodos que utiliza para analisar ficheiros no seu computador são determinados pelas propriedades atribuídas a cada tarefa.

Para configurar as definições da tarefa:

Abra a janela principal de definições e seleccione o nome da tarefa por baixo de **Verificar**.

Pode utilizar a janela de definições para cada tarefa para:

- Seleccionar um nível de segurança com as definições que a tarefa utilizará (ver 14.4.1 na pág. 209)
- Editar as definições avançadas:
    - as definições que definem os tipos de ficheiros que devem ser analisados (ver 14.4.2 na pág. 210)
    - configurar o início da tarefa, utilizando um perfil de utilizador diferente (ver 6.4 na pág. 87)

- configurar definições de verificação avançadas (ver 14.4.5 na pág. 216)
- Restaurar as definições de verificação predefinidas (ver 14.4.3 na pág. 214)
- Seleccionar uma acção que o programa aplicará quando detectar um ficheiro infectado ou suspeito (ver 14.4.4 na pág. 214)
- Criar um agendamento (ver 6.5 na pág. 88) para executar as tarefas automaticamente
- Além disso, pode configurar as definições globais (ver 14.4.6 na pág. 218) para a execução de todas as tarefas

As secções que se seguem irão examinar, em detalhe, as definições de tarefa acima listadas.

14.4.1. Seleccionar um nível de segurança

Cada tarefa de verificação de vírus analisa objectos num destes níveis (ver Figura 64):

Elevado – a verificação completa do computador ou dos discos, pastas ou ficheiros. Recomendamos este nível se suspeita que um vírus infectou o seu computador.

Recomendado. Os especialistas da Kaspersky Lab recomendam este nível. A verificação funciona de modo igual ao nível **Elevado**, excepto nos ficheiros de correio electrónico.

Baixo – nível com definições que o deixam utilizar, confortavelmente, as aplicações de recursos intensivos, já que o âmbito dos ficheiros analisados é reduzido.

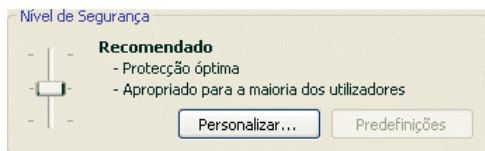



Figura 64. Seleccionar o nível de segurança da verificação de vírus

Por definição, o nível de verificação de ficheiros está configurada no nível **Recomendado**.

Você pode aumentar ou diminuir o nível de segurança de verificação seleccionando o nível que deseja ou alterando as definições para o nível actualmente seleccionado.

Para alterar o nível de segurança:

Ajuste os indicadores. Ao ajustar o nível de segurança, você define o rácio da velocidade de verificação para o número total de ficheiros analisados: quanto menos ficheiros forem analisados, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de ficheiros listados responder às suas necessidades, pode personalizar as definições de verificação. Para o fazer, seleccione o nível que está mais próximo das sua necessidades como ponto de partida e edite as suas definições. Se o fizer, o nível será denominado como **Definições Personalizadas**.

Para modificar as definições para um nível de segurança:

Clique no botão **Personalizar** na janela de definições da tarefa. Edite as definições de verificação na janela que se abrir e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Definições Personalizadas** que contém as definições de verificação que você configurou.

14.4.2. Definir os tipos de objectos a verificar

Ao especificar os tipos de objectos a analisar, você estabelece que tipo de ficheiros, tamanhos e unidades serão analisados quando a tarefa estiver a funcionar.

Os tipos de ficheiros analisados são definidos na secção **Tipos de Ficheiros** (ver Figura 65). Seleccionar uma das três opções:

- **Verificar todos os ficheiros**. Com esta opção, todos os objectos serão analisados sem excepção.
- **Programas e documentos (por conteúdo)**. Se seleccionar este grupo de programas, só serão analisados ficheiros potencialmente infectados – ficheiros nos quais um vírus se poderá ter introduzido.

Nota:

Existem alguns formatos de ficheiros que têm um risco relativamente reduzido de possuírem código malicioso inserido neles e, subsequentemente, ser activado. Um exemplo são os ficheiros txt.

Por outro lado, existem formatos de ficheiros que contém ou podem conter código executável. Os exemplos são os formatos .exe, .dll, ou .doc. Nesses ficheiros, o risco de inserção e activação de código malicioso é relativamente elevado.

Antes de procurar vírus num ficheiro, o seu cabeçalho interno é analisado para determinar o formato do ficheiro (txt, doc, exe, etc.).

Programas e documentos (por extensão). Neste caso, o programa só analisará ficheiros potencialmente infectados e, ao fazê-lo, o formato do ficheiro será determinado pela extensão. Utilizando a ligação Extensões, pode rever uma lista das extensões de ficheiros que são analisados com esta opção (ver A.1 na pág. 329).

Dica:

Não se esqueça que alguém pode enviar um vírus para o seu computador com a extensão .txt, que é na realidade um ficheiro executável renomeado como um ficheiro .txt. Se seleccionar a opção **Programas e documentos (por extensão)**, tal ficheiro seria ignorado pela verificação. Se a opção **Programas e documentos (por conteúdo)** for seleccionada, ignorando as extensões, o programa analisará cabeçalhos dos ficheiros, revelando que o ficheiro é, de facto, um ficheiro .exe. Tal ficheiro seria verificado em profundidade, quanto à existência de vírus.

Na secção **Produtividade**, pode especificar que apenas serão verificados os ficheiros novos e aqueles que foram modificados desde a última verificação. Este modo reduz, notavelmente, o tempo de análise e aumenta a velocidade de desempenho do programa. Para o fazer, deve seleccionar a opção **Verificar apenas os ficheiros novos e modificados**. Este modo estende-se aos ficheiros simples e compostos.

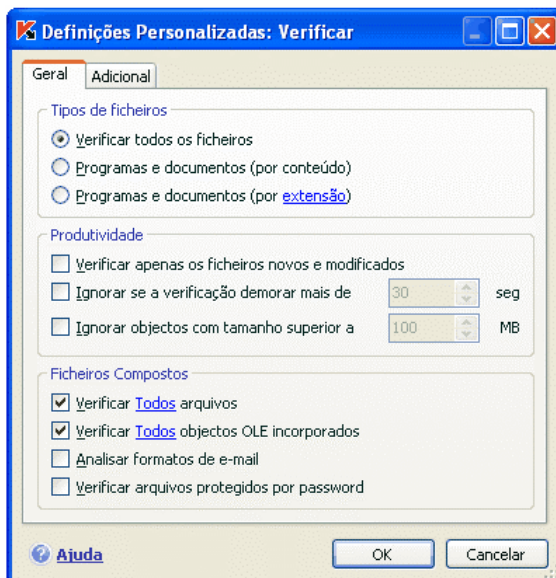



Figura 65. Configurar definições de verificação

Na secção **Produtividade,** também pode estabelecer limites de tempo e de tamanho para os ficheiro a verificar.

☑ **Ignorar se a verificação demorar mais de ... segundos.** Seleccione esta opção e introduza o tempo de verificação máximo para um ficheiro. Desse modo, se este tempo for excedido, este ficheiro será removido da fila da verificação.

☑ **Ignorar objectos com tamanho superior a ... MB**. Seleccione esta opção e introduza o tamanho máximo para um ficheiro. Desse modo, se o tamanho for excedido, este ficheiro será removido da fila da verificação.

Na secção **Ficheiros Compostos**, especifique que ficheiros compostos devem ser verificados:

☑ **Verificar Todos / Apenas novos arquivos** – verifica os arquivos .rar, .arj, .zip, .cab. .lha, .jar, e .ice.

Aviso!

O Kaspersky Anti-virus não apaga automaticamente formatos de ficheiros comprimidos que não suporta (por exemplo, .ha, .uue, .tar), mesmo se tiver seleccionado a opção para tratar automaticamente ou eliminar se os objectos não puderem ser tratados.

Para apagar esses ficheiros comprimidos, clique na ligação Apagar arquivos na janela de aviso sobre a detecção do objecto perigoso. Este aviso será apresentado no ecrã depois do programa começar a processar os objectos detectados durante a verificação. Também pode apagar manualmente os ficheiros infectados.

☑ **Verificar Todos / Apenas novos objectos OLE incorporados** – verifica os objectos incorporados nos ficheiros (por exemplo, as folhas de cálculo do Excel ou uma macro incorporada num ficheiro do Microsoft Word, anexos de correio electrónico, etc.).

Para cada tipo de ficheiros compostos, pode seleccionar e analisar todos os ficheiros ou só os novos. Para o fazer, utilize a ligação junto ao nome dos ficheiros. Isto alterará o seu valor quando clicar nela com o botão esquerdo do rato. Se a secção **Produtividade** foi configurada para só analisar ficheiros novos ou modificados, você apenas poderá seleccionar o tipo de ficheiros compostos a serem verificados.

☑ **Analisar formatos de e-mail** – analisa ficheiros de e-mails e bases de dados de e-mails. Se caixa estiver seleccionada, o Kaspersky Anti-virus irá analisar o ficheiro de e-mail e cada componente do e-mail (corpo, os anexos) em termos de vírus. Se esta caixa não estiver seleccionada, o ficheiro de e-mail será analisado como um objecto único.

Repare nestes pontos de verificação de bases de dados de correio electrónico protegidas por palavra-passe:

- O Kaspersky Anti-Virus para Windows Workstations detecta código malicioso na base de dados do Microsoft Office Outlook 2000 mas não o trata;
- O Kaspersky Anti-Virus para Windows Workstations não suporta análises de código malicioso nas bases de dados protegidas do Microsoft Office Outlook 2003.

☑ **Verificar arquivos protegidos por password** – verifica os arquivos protegidos por password. Com esta funcionalidade, uma janela pedirá uma password perante os ficheiros arquivados analisados. Se esta caixa não estiver seleccionada, os arquivos protegidos por password não serão analisados.

14.4.3. Restaurar as definições de verificação predefinidas

Ao configurar as definições das tarefas de verificação, você pode sempre retornar às definições recomendadas. A Kaspersky Lab considera-as as mais adequadas e combinou-as no nível de segurança **Recomendado**.

Para restaurar as predefinições das verificações de vírus:

1. Seleccione o nome da tarefa na secção **Verificar** da janela principal e use a ligação Definições para abrir a janela de definições da tarefa.
2. Clique no botão **Predefinições** na secção **Nível de Segurança**.

14.4.4. Seleccionar acções para objectos

Quando, ao verificar um ficheiro quanto à existência de vírus, se descobrir que o mesmo está infectado ou se suspeitar que está infectado, as acções subsequentes do programa dependem do estado dos objectos e da acção seleccionada.

Uma dos seguintes estados podem ser atribuídos a um ficheiro depois da verificação:

- Programa malicioso (por exemplo, *vírus, Trojan*).
- *Potencialmente infectado,* quando a verificação não consegue determinar se o objecto está infectado. Isto significa que o código do ficheiro contém uma secção de código que se assemelha a um vírus conhecido mas alterado ou que faz lembrar a estrutura de uma sequência de vírus.

Por defeito, todos os ficheiros infectados são sujeitos à desinfecção e, se estiverem potencialmente infectados, são enviados para a Quarentena.

Para editar uma acção para um objecto:

seleccione o nome da tarefa na secção **Verificar** da janela principal do programa e utilize a ligação Definições para abrir a janela de definições da tarefa. Todas as acções possíveis são apresentadas nas secções apropriadas (ver Figura 66).

Figura 66. Seleccionar acções para ficheiros perigosos

Se a acção seleccionada foi	Quando detecta um objecto malicioso ou potencialmente infectado
Perguntar o que fazer quando a verificação for concluída	O programa não processa os ficheiros antes do fim da verificação. Quando a verificação está completa, a janela das estatísticas aparecerá com uma lista de ficheiros detectados e ser-lhe-á perguntado se quer processar os objectos.
Perguntar o que fazer durante a verificação	O programa emitirá uma mensagem de aviso que contém informação sobre o código malicioso que infectou ou infectou possivelmente o ficheiro e dá-lhe a escolher uma das seguintes acções.
Não perguntar o que fazer	O programa grava informação sobre os ficheiros detectados no relatório, sem os ter processado ou notificado o utilizador. Não recomendamos que utilize esta funcionalidade, já que os ficheiros infectados permanecem no seu computador e é, praticamente impossível, evitar a infecção.

Se a acção seleccionada foi	Quando detecta um objecto malicioso ou potencialmente infectado
Não perguntar o que fazer ☑ **Desinfectar**	O programa tenta tratar o objecto detectado sem pedir a confirmação ao utilizador. Se a desinfecção falhar, será atribuído o estado de *potencialmente infectado* ao ficheiro e este será movido para a Quarentena (ver 17.1 na pág. 239). A informação acerca disto é gravada no relatório (ver 17.3 na pág. 245). Mais tarde, você pode tentar desinfectar este objecto.
Não perguntar o que fazer ☑ **Desinfectar** ☑ **Apagar se a desinfecção falhar**	O programa tenta tratar o ficheiro detectado sem pedir a confirmação ao utilizador. Se o ficheiro não puder ser desinfectado, o mesmo é apagado.
Não perguntar o que fazer ☐ **Desinfectar** ☑ **Apagar**	O programa apaga o ficheiro automaticamente.

Antes de tentar desinfectar ou apagar um objecto, o Kaspersky Anti-virus para Windows Workstations cria uma cópia de segurança e envia-a para a Cópia de Segurança (ver 17.2 na pág. 243) caso o objecto precise de ser restaurado ou surja uma oportunidade de o tratar.

14.4.5. Definições avançadas de verificação de vírus

Para além de configurar as definições básicas da verificação de vírus, também pode utilizar as definições avançadas (ver Figura 67):

☑ **Activar tecnologia iChecker** – utiliza a tecnologia que pode aumentar a velocidade de verificação, excluindo determinados objectos da verificação. Um objecto é excluído da verificação, utilizando um algoritmo especial que toma em consideração a data de distribuição das assinaturas de ameaças, a data em que o objecto foi verificado pela última vez e as alterações às definições de verificação.

Por exemplo, você tem um arquivo que o programa analisou e atribuiu a classificação de *não infectado*. Na próxima vez, o programa vai ignorar este arquivo, a menos que este seja modificado ou as definições alteradas. Se a estrutura do arquivo mudar porque foi adicionado um novo ficheiro, se as definições de verificação foram alteradas ou se as assinaturas de ameaças foram actualizadas, o programa analisará o arquivo novamente. Existem limitações no iChecker™: não funciona com ficheiros extensos e apenas se aplica a ficheiros com uma estrutura que o Kaspersky Anti-virus para Windows Workstations reconheça (por exemplo, *.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar*).

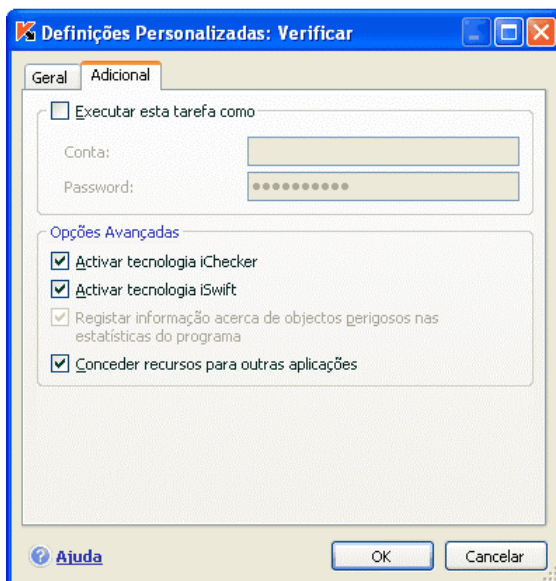



Figura 67. Definições avançadas de verificação

☑ **Activar tecnologia iSwift** – Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam sistemas de ficheiros NTFS. Existem algumas limitações no iSwift™: está limitado a um local específico para o ficheiro no sistema de ficheiros e aplica-se apenas a objectos em sistemas de ficheiros NTFS.

> A tecnologia iSwift não está disponível nos computadores que funcionam com o Microsoft Windows 98SE/ME/XP64.

☑ **Registar informação acerca de objectos perigosos nas estatísticas do programa** – Guarda informação acerca dos objectos perigosos detectados nas estatísticas gerais do programa e apresenta uma lista das ameaças

detectadas durante a verificação no separador **Detectadas** da janela de relatório (ver 17.3.2 na pág. 249). Se esta opção estiver desactivada, a informação acerca de objectos perigosos não será apresentada no relatório e será impossível processar os dados.

☑ **Conceder recursos para outras aplicações** – pausa aquela tarefa de verificação de vírus se o processador estiver ocupado com outras aplicações.

14.4.6. Estabelecer definições globais para todas as tarefas de verificação

Cada tarefa de verificação é executada de acordo com as suas próprias definições. Por definição, as tarefas criadas, quando você instalou o programa no seu computador, utilizam as definições recomendadas pelos especialistas da Kaspersky Lab.

Você pode configurar as definições globais para todas as tarefas de verificação. Como ponto de partida, você utilizará um conjunto de propriedades utilizadas para procurar vírus num ficheiro individual.

Para atribuir definições globais para todas as tarefas de verificação:

1. Na janela principal no programa, na zona esquerda, seleccione a secção **Verificar** e clique em Definições.
2. Na janela que é aberta, configure as definições da verificação: seleccione o nível de segurança (ver 14.4.1 na pág. 209), configure as definições de nível avançado e seleccione uma acção para objectos (ver 14.4.4 na pág. 214).
3. Para aplicar estas novas definições a todas as tarefas, clique no botão **Aplicar** na secção **Outras definições de tarefa**. Confirme a definições globais que seleccionou na caixa de dialogo que aparece.

CAPÍTULO 15. TESTAR AS FUNÇÕES DO KASPERSKY ANTI-VIRUS

Depois de instalar e configurar o Kaspersky Anti-virus, recomendamos que verifique se as definições e o funcionamento do programa estão correctos, usando um vírus de teste e variantes do mesmo.

15.1. O vírus de teste EICAR e as suas variantes

O vírus de teste foi, especialmente, desenvolvido pelo eicar (O Instituto Europeu para Pesquisa de Antivírus de Computador) para testar a funcionalidade de anti-vírus.

O vírus de teste NÃO É UM VÍRUS e não contém código de programa que possa danificar o seu computador. Contudo, a maioria dos programas de anti-vírus identificá-lo-á como um vírus.

Nunca use vírus reais para testar a funcionalidade de um anti-vírus!

Pode transferir um vírus de teste a partir do site oficial do **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

O ficheiro que transferiu do site do **EICAR** contém o corpo de um vírus de teste padrão. O Kaspersky Anti-virus irá detectá-lo, classificá-lo como um **vírus** e tomar a acção definida para aquele tipo de objecto.

Para testar as reacções do Kaspersky Anti-virus quando são detectados diferentes tipos de objectos, você pode alterar os conteúdos do vírus de teste padrão, adicionando um dos prefixos apresentados na tabela que se segue.

Prefixo	Estado do vírus de teste	Acção correspondente quando a aplicação processa o objecto
Sem prefixo, vírus de teste padrão	O ficheiro contém um vírus de teste. Não é possível desinfectar o objecto.	A aplicação identificará o objecto como malicioso, não sujeito a tratamento e irá apagá-lo.

Prefixo	Estado do vírus de teste	Acção correspondente quando a aplicação processa o objecto
CORR-	Corrompido.	A aplicação conseguia aceder ao objecto, mas não consegui verificá-lo, uma vez que o objecto está corrompido (por exemplo, a estrutura de ficheiro foi violada ou é um formato inválido).
SUSP- WARN-	O ficheiro contém um vírus de teste (variante). Não é possível desinfectar o objecto.	Este objecto é uma variante de um vírus conhecido ou um vírus desconhecido. Na altura da detecção, as bases de dados de assinaturas de ameaças não contêm uma descrição do procedimento para tratar este objecto. A aplicação colocará o objecto em Quarentena para ser processado mais tarde com assinaturas de ameaças actualizadas.
ERRO-	Erro de processamento.	Ocorreu um erro ao processar o objecto: a aplicação não consegue aceder ao objecto que está a ser verificado, uma vez que a integridade do objecto foi violada (por exemplo, não há fim para um arquivo multi-volume) ou existe ligação para o mesmo (se o objecto está a ser analisado numa unidade de rede).
CURE-	O ficheiro contém um vírus de teste. É possível tratá-lo. O objecto é sujeito a desinfecção e o texto do corpo do vírus alterar-se-á para CURE.	O objecto contém um vírus que pode ser tratado. A aplicação analisará o objecto em termos de vírus, após o qual este será completamente tratado.

Prefixo	Estado do vírus de teste	Acção correspondente quando a aplicação processa o objecto
DELE–	O ficheiro contém um vírus de teste. Não é possível desinfectar o objecto.	Este objecto contém um vírus que não pode ser desinfectado ou é um Trojan. A aplicação apaga estes objectos.

A primeira coluna da tabela contém os prefixos que é necessário adicionar ao início da sequência para um vírus de teste padrão. A segunda coluna descreve o estado e reacção do Kaspersky Anti-virus aos vários tipos de vírus de teste. A terceira coluna contém informação sobre objectos com o mesmo estado que a aplicação processou.

Os valores presentes nas definições de verificação anti-vírus determinam a acção tomada em cada um dos objectos.

15.2. Testar o Anti-vírus de Ficheiros

Para testar a funcionalidade do Anti-vírus de Ficheiros;

1. Crie uma pasta num disco, copie para essa pasta o vírus de teste transferido a partir do site oficial da organização (ver 15.1 na pág. 219) e as variantes do vírus de teste que você criou.
2. Permita que todos os eventos sejam registados para que o ficheiro relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros. Para o fazer assinale a opção ☑ **Registar eventos não críticos** na janela das definições do relatório.
3. Execute o vírus de teste ou uma variante do mesmo.

O Anti-vírus de Ficheiros irá interceptor a sua tentativa para aceder ao ficheiro, irá verificá-lo e informá-lo-á de que detectou um objecto perigoso:

Quando selecciona diferentes opções para lidar com os objectos detectados, pode testar as reacções do Anti-vírus de Ficheiros à detecção de vários tipos de objectos.

Pode ver os detalhes sobre o desempenho do Anti-vírus de Ficheiros no relatório da componente.

15.3. Testar as tarefas de verificação de vírus

Para testar tarefas de verificação de vírus:

1. Crie uma pasta num disco, copie para essa pasta o vírus de teste transferido a partir do site oficial da organização (ver 15.1 na pág. 219) e as variantes do vírus de teste que você criou.

2. Crie uma nova tarefa de verificação de vírus (ver 14.3 na pág. 207) e seleccione a pasta com o conjunto de vírus de teste como os objectos a verificar (ver 14.2 na pág. 205).

3. Permita que todos os eventos sejam registados para que o ficheiro relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros. Para o fazer assinale a opção ☑ **Registar eventos não críticos** na janela das definições do relatório.

4. Execute a tarefa de verificação de vírus (ver 14.1 na pág. 205).

Quando executa uma verificação, como são detectados objectos suspeitos ou infectados, são apresentadas notificações no ecrã com informação acerca dos objectos, perguntando ao utilizador qual a próxima acção a tomar:

Desta forma, ao seleccionar diferentes opções para as acções, pode testar as reacções do Kaspersky Anti-virus à detecção de diferentes tipos de objectos.

Pode ver os detalhes sobre o desempenho de uma tarefa de verificação de vírus no relatório da componente.

CAPÍTULO 16. ACTUALIZAÇÕES DO PROGRAMA

Manter o seu software anti-vírus actualizado é um investimento na segurança do seu computador. É importante actualizar regularmente a aplicação de forma a manter a sua informação constantemente protegida, porque novos vírus e novo software malicioso surgem diariamente.

Actualizar a aplicação envolve a transferência e instalação das seguintes componentes no seu computador:

- **Assinaturas de ameaças, assinaturas de ataques de rede e controladores de rede**

  A informação no seu computador é protegida utilizando uma base de dados que contém assinaturas de ameaças e perfis de ataques de rede. As componentes de protecção que fornecem a protecção utilizam a base de dados de assinaturas de ameaças para procurar e desinfectar objectos perigosos no seu computador. As assinaturas são actualizadas todas as horas com novas ameaças e métodos de como as combater. Por isso, recomenda-se que elas sejam actualizadas regularmente.

  Para além das assinaturas de ameaças e a base de dados de ataques de rede, também são actualizados os controladores de rede que permitem que as componentes de protecção interceptem o tráfego de rede.

  As versões anteriores das aplicações da Kaspersky Lab englobavam conjuntos de bases de dados padrão e alargadas. Cada uma delas tratava de proteger o seu computador em relação a tipos diferentes de ficheiros perigosos. No Kaspersky Anti-Virus para Windows Workstations não precisamos de nos preocupar com a selecção do conjunto apropriado de assinaturas de ameaças. Agora, os nossos produtos utilizam as assinaturas de ameaças que o protegem tanto dos ficheiros maliciosos e potencialmente perigosos variados como dos ataques de hackers.

- **Módulos do programa**

  Além das assinaturas, pode actualizar os módulos internos do Kaspersky Anti-virus. Surgem, regularmente, novas actualizações da aplicação.

A origem principal de actualização para o Kaspersky Anti-virus para Windows Workstations são os servidores de actualização da Kaspersky Lab.

Para transferir as actualizações disponíveis a partir dos servidores de actualização, o seu computador tem de estar ligado à Internet.

Se não tiver acesso aos servidores de actualização da Kaspersky Lab (por exemplo, o seu computador não está ligado à Internet), pode ligar para a sede da Kaspersky Lab +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 para pedir informação de contacto dos parceiros da Kaspersky Lab que lhe possam fornecer actualizações comprimidas em disquetes ou CDs.

As actualizações podem ser transferidas através de um dos seguintes modos:

- *Automaticamente.* O Kaspersky Anti-virus verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização. As verificações podem ser definidas para serem mais frequentes durante surtos de vírus e menos frequentes quando esses surtos terminam. Quando o Anti-vírus detecta novas actualizações, transfere-as e instala-as no computador. Esta é a opção predefinida.
- *De acordo com agendamento*. A actualização está estipulada para começar numa altura específica.
- *Manualmente.* Com esta opção, você inicializa manualmente o Actualizador.

Durante a actualização, a aplicação compara as assinaturas de ameaças e os módulos da aplicação existentes no seu computador com as versões disponíveis no servidor de actualização. Se o seu computador tiver a última versão das assinaturas e módulos da aplicação, visualizará uma janela de notificação confirmando que o seu computador está actualizado. Se as assinaturas e módulos existentes no seu computador e no servidor de actualizações diferirem, a aplicação só transferirá as partes que faltam das actualizações. O Actualizador não transfere assinaturas e módulos que você já tenha, o que aumenta, significativamente, a velocidade de transferência e poupa tráfego de Internet.

Antes de actualizar as assinaturas de ameaças, o Kaspersky Anti-virus para Windows Workstations cria cópias de segurança das mesmas, que podem ser utilizadas se for necessário reverter para a última versão das assinaturas (ver 16.2 na pág. 226). Se, por exemplo, o processo de actualização corrompe as assinaturas de ameaças e deixa-as inutilizáveis, você pode facilmente reverter para a versão anterior e tentar actualizar as assinaturas mais tarde.

Você pode distribuir as actualizações para uma origem local ao mesmo tempo que actualiza a aplicação (ver 16.4.4 na pág. 235). Esta função permite-lhe actualizar bases de dados e módulos usados pelas aplicações da versão 6.0 em computadores de rede para poupar na largura de banda.

16.1. Iniciar o Actualizador

Pode começar o processo de actualização em qualquer altura. Este funcionará a partir da origem de actualização que você seleccionar (ver 16.4.1 na pág. 228).

Pode iniciar o Actualizador a partir do:

- menu de contexto (ver 4.2 na pág. 53).
- janela principal do programa (ver 4.3 na pág. 55)

Para iniciar o Actualizador a partir do menu de contexto:

1. Clique com o botão direito do rato no ícone da aplicação na bandeja do sistema para abrir o menu de contexto.
2. Seleccione **Actualização**.

Para iniciar o Actualizador a partir da janela principal do programa:

1. Seleccione **Actualização** na secção **Serviço**.
2. Clique em **Actualizar agora!** no painel direito da janela principal ou utilize o botão ▶ da barra de estado.

O progresso da actualização será exibido numa janela especial. Pode esconder a janela de progresso de actualização. Para o fazer, clique em **Fechar**. A actualização continuará com a janela escondida.

Note que as actualizações são distribuídas na origem local durante o processo de actualização, desde que este serviço esteja activado (ver 16.4.4 na pág. 235).

16.2. Reverter para a actualização anterior

Sempre que iniciar o Actualizador, o Kaspersky Anti-virus para Windows Workstations primeiro cria uma cópia de segurança das actuais assinaturas de ameaças e só depois inicia a transferência das actualizações. Desta forma, você pode voltar a utilizar a versão anterior das assinaturas se a actualização falhar.

Para voltar à versão anterior das assinaturas de ameaças:

1. Seleccione a componente **Actualização** na secção **Serviço** na janela principal do programa.
2. Clique no botão **Reversão** no painel direito da janela principal do programa.

16.3. Criar tarefas de actualização

O Kaspersky Anti-virus tem integrada uma tarefa de actualização para actualizar módulos do programa e assinaturas de ameaças. Também pode criar as suas próprias tarefas de actualização com várias definições e agendamentos.

Por exemplo, você instalou o Kaspersky Anti-virus num portátil que usa em casa e no trabalho. Em casa, você actualiza o programa a partir dos servidores de actualização da Kaspersky Lab e no trabalho actualiza a partir de uma pasta local que guarda as actualizações de que necessita. Utilize duas tarefas diferentes para evitar ter que mudar as definições de actualização sempre que muda de local.

Para criar uma tarefa de actualização avançada:

1. Seleccione **Actualização** na secção **Serviço** da janela principal do programa, abra o menu de contexto, clicando com o botão direito, e seleccione **Guardar como**.
2. Insira o nome para a tarefa na janela que se abre e clique em **OK**. Aparecerá uma tarefa com esse nome na secção **Serviço** da janela principal do programa.

Aviso!

Existe um limite para o número de tarefas de actualização que o utilizador pode criar no Kaspersky Anti-Virus. O número máximo é duas tarefas.

A nova tarefa herda todas as propriedades da tarefa na qual se baseou para criar a nova tarefa, excepto no que diz respeito às definições de agendamento. Para esta nova tarefa, é desactivada a definição de verificação automática que existe por defeito.

Depois de criar uma tarefa, configure definições avançadas: especifique a origem de actualização (ver 16.4.1 na pág. 228), as definições de ligação de rede (ver 16.4.3 na pág. 233) e, se necessário, active as tarefas com outro perfil (ver 6.4 na pág. 87) e configure o horário agendado (ver 6.5 na pág. 88).

Para mudar o nome de uma tarefa:

Seleccione a tarefa na secção **Serviço** da janela principal do programa, abra o meu de contexto, clicando com o botão direito do rato, e seleccione **Mudar nome**.

Insira o novo nome para a tarefa na janela que se abre e clique em **OK**. O nome da tarefa será então alterado na secção **Serviço**.

Para apagar uma tarefa:

Seleccione a tarefa na secção **Serviço** da janela principal do programa, abra o menu de contexto, clicando com o botão direito do rato, e seleccione **Apagar**.

Na janela de confirmação, confirme que pretende apagar a tarefa. A tarefa será então apagada da lista de tarefas na secção **Serviço**.

Aviso!

Apenas pode alterar o nome e apagar tarefas que foram criadas por si.

16.4. Configurar as definições de actualização

As definições do Actualizador especificam os seguintes parâmetros:

- A origem a partir da qual são transferidas e instaladas as actualizações (ver 16.4.1 na pág. 228);
- O modo de actualização da aplicação e os itens específicos actualizados (ver 16.4.2 na pág. 231);
- A frequência de actualização se as actualizações são executadas com um agendamento (ver 6.5 na pág. 88);
- A conta de utilizador com a qual será executada a actualização (ver 6.4 na pág. 87);
- O requisito para copiar actualizações transferidas para um directório local (ver 16.4.4 na pág. 235);
- Quais as acções que deve efectuar depois de concluída a actualização (ver 16.4.5 na pág. 236).

As secções que se seguem irão examinar, em detalhe, estes aspectos.

16.4.1. Seleccionar uma origem de actualização

A *origem de actualização* é um recurso que contém as actualizações para as assinaturas de ameaças e para os módulos da aplicação do Kaspersky Anti-Virus.

Pode usar as seguintes origens de actualização:

- *Servidor de Administração* – uma área centralizada para armazenamento de actualizações, localizada no Servidor de Administração do Kaspersky Administration Kit (para mais detalhes, veja o Manual de Utilização do Administrador do Kaspersky Administration Kit).
- *Servidores de actualização da Kaspersky Lab* – sites especiais que contêm as actualizações disponíveis para as assinaturas de ameaças e módulos da aplicação de todos os produtos da Kaspersky Lab.
- *Servidor de HTTP ou FTP ou pasta local ou de rede* – servidor ou pasta local que contém as últimas actualizações.

Se não tiver acesso aos servidores de actualização da Kaspersky Lab (por exemplo, não possui ligação à Internet), pode ligar para a sede da Kaspersky Lab +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 para pedir informação de contacto dos parceiros da Kaspersky Lab que lhe possam fornecer actualizações comprimidas em disquetes ou CDs.

> Aviso!
>
> Ao solicitar actualizações em meios removíveis, por favor especifique se também deseja as actualizações para os módulos internos da aplicação.

Pode copiar as actualizações a partir de um disco e transferi-las para um site FTP ou HTTP ou guardá-las numa pasta local ou da rede.

Seleccione a origem da actualização no Separador **Origem da actualização** (ver Figura 68).

Por defeito, as actualizações são transferidas a partir dos servidores de actualização dos servidores da Kaspersky Lab. A lista de endereços que este item representa não pode ser editada. Ao actualizar, o Kaspersky Anti-virus para Windows Workstations chama esta lista, selecciona o endereço do primeiro servidor e tenta transferir os ficheiros a partir desse servidor. Se as actualizações não poderem ser transferidas a partir do primeiro servidor, a aplicação tenta ligar-se a cada um dos servidores seguintes até ser bem sucedida.

Para transferir actualizações de outro site FTP ou HTTP:

1. Clique em **Adicionar.**
2. Na caixa de diálogo **Seleccionar origem de actualização**, seleccione o site alvo FTP ou HTTP ou especifique, no campo **Origem,** o endereço IP, nome do caractere ou endereço URL deste site. Ao seleccionar um site ftp como uma origem de actualização, as definições de autenticação devem ser inseridas no URL do servidor com o seguinte formato ftp://user:password@server.

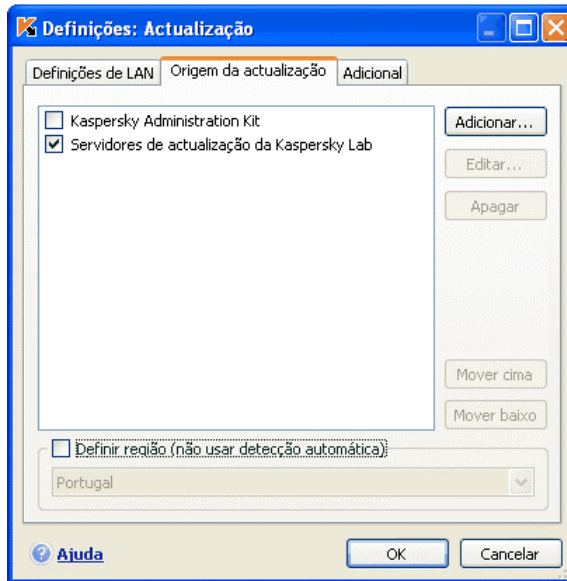



Figura 68. Seleccionar uma origem da actualização

Aviso!

Se seleccionou um recurso localizado fora da LAN (Rede de Área Local) como uma origem de actualização, então necessita de uma ligação à Internet para recolher as actualizações.

Para actualizar a partir de uma pasta local:

1. Clique **Adicionar.**
2. Na caixa de diálogo **Seleccionar origem de actualização**, seleccione uma pasta ou especifique o atalho completo para esta pasta no campo **Origem**.

O Kaspersky Anti-Virus para Windows Workstations adiciona uma nova origem de actualização ao topo da lista e assinala, automaticamente, esta origem como estando activada, assinalando a caixa junto ao nome da origem.

Se vários recursos são seleccionados como origens de actualização, a aplicação tenta ligar-se a eles um após o outro, começando no topo da lista e restabelece as actualizações a partir da primeira origem disponível. Pode alterar a ordem das origens na lista, utilizando os botões **Mover cima** e **Mover baixo**.

Para editar esta lista, utilize os botões **Adicionar**, **Editar** e **Apagar.** A única origem que não poderá editar ou apagar é a origem relativa aos servidores de actualização da Kaspersky Lab.

Se utilizar os servidores de actualização da Kaspersky Lab como origem de actualização, pode seleccionar a localização optimizada do servidor para transferir actualizações. A Kaspersky Lab possui servidores em vários países. Ao escolher o servidor de actualização da Kaspersky Lab mais próximo de si, poupa tempo e efectuará mais rapidamente as transferências de actualizações.

Para escolher o servidor mais próximo, seleccione ☑ **Definir região (não usar detecção automática)** e seleccione o país mais próximo da sua actual localização a partir da lista pendente. Se assinalar esta caixa, as actualizações serão executadas tendo em consideração a região seleccionada na lista. Por defeito, esta caixa está desmarcada e é usada a informação acerca da actual região do registo do sistema operativo.

16.4.2. Seleccionar o método de actualização e o que actualizar

Ao configurar as definições de actualização, é importante definir o que actualizar e qual o método de actualização a utilizar.

Os <u>objectos de actualização</u> (ver Figura 69) são as componentes a serem actualizadas:

- assinaturas de ameaças
- controladores de rede que permitem que as componentes de protecção interceptem o tráfego de rede
- Bases de dados de ataques de rede utilizadas pelo Anti-Hacker
- módulos do programa

As assinaturas de ameaças, controladores de rede e bases de dados de ataques de rede são sempre actualizadas, enquanto os módulos da aplicação só são actualizados se for seleccionado o respectivo modo.

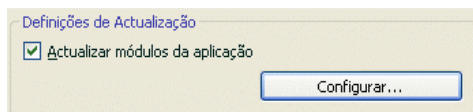



Figura 69. Seleccionar objectos de actualização

Se deseja transferir e instalar actualizações para os módulos do programa:

Seleccione ☑ **Actualizar módulos da aplicação** na caixa de diálogo **Definições de Actualização** do serviço **Actualização**.

Se existir uma actualização dos módulos da aplicação na origem de actualização, a aplicação transferirá as actualizações necessárias e aplicá-las-á depois do sistema ser reiniciado. As actualizações dos módulos transferidas só serão instaladas depois do computador ser reiniciado.

Se a próxima actualização do programa acontecer antes do computador ser reiniciado e antes das actualizações dos módulos do programa anteriormente transferidas serem instaladas, só serão actualizadas as assinaturas de ameaças.

O Método de Actualização (ver Figura 70) define como é que o Actualizador é iniciado. Pode escolher um destes métodos na secção **Modo de Execução**:

◉ **Automaticamente** – O Kaspersky Anti-virus verifica, em intervalos especificados, se existem actualizações na origem de actualização. Se encontrar novas actualizações, o Anti-vírus transfere-as e instala-as no computador. Este modo é utilizado por predefinição.

Se um recurso de rede for especificado como origem de actualização, o Kaspersky Anti-virus para Windows Workstations tenta iniciar a actualização depois de um determinado período de tempo, conforme o especificado no anterior pacote de actualização. Se for seleccionada uma pasta local como origem de actualização, a aplicação tenta transferir as actualizações a partir da pasta local com a frequência especificada no pacote de actualização transferido durante a última actualização. Esta opção permite à Kaspersky Lab regular a frequência de actualização do programa no caso de surtos de vírus aparecer e noutras situações potencialmente perigosas. A sua aplicação receberá as últimas actualizações para as assinaturas de ameaças, ataques de rede e módulos do software de forma atempada, prevenindo desta forma a entrada de software malicioso no seu computador.

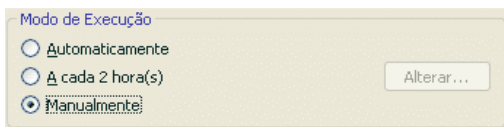



Figura 70. Seleccionar o modo de execução das actualizações

◉ **Segundo agendamento**. A actualização está agendada para começar num momento especificado. Por defeito, as actualizações agendadas ocorrerão a cada 2 horas. Para editar o agendamento predefinido, clique no botão **Alterar...** junto ao título do modo e faça as alterações necessárias na janela que se abre (para mais detalhes, ver 6.5 na pág. 88).

Manualmente. Com esta opção, inicia manualmente o Actualizador. O Kaspersky Anti-virus para Windows Workstations notifica-o quando precisa de o actualizar:

- Em cima do ícone de bandeja do sistema, aparece uma mensagem a informá-lo de que a actualização é necessária (se os avisos estiverem activados; ver 17.11.1 na pág. 278)
- O segundo indicador na janela principal do programa informa-o de que o seu computador está desactualizado (ver 5.1.1 na pág. 60)
- Surge uma recomendação para actualização da aplicação na secção de mensagens na janela principal do programa (ver 4.3 na pág. 55)

16.4.3. Configurar as definições de ligação de rede

Se configurar o programa para ir buscar actualizações aos servidores de actualização da Kaspersky Lab ou a outros sites FTP ou HTTP, recomendamos que verifique primeiro as suas definições de ligação de rede.

Todas as definições estão agrupadas num separador especial – **Definições de LAN** (ver Figura 71).

Seleccione **Utilizar modo FTP passivo se possível** se transferir as actualizações a partir de um servidor FTP em modo passivo (por exemplo, através de uma firewall). Se estiver a trabalhar em modo FTP activo, desmarque esta caixa de selecção.

No campo **Tempo limite de ligação … (seg)**, defina o tempo atribuído para a ligação ao servidor de actualização. Se a ligação falhar, depois deste tempo ter decorrido o programa tentará ligar-se ao próximo servidor de actualização. Isto continua até que seja estabelecida uma ligação com sucesso ou até tentar todos os servidores de actualização disponíveis.

Seleccione **Utilizar servidor de proxy** se estiver a utilizar um servidor de proxy para aceder à Internet e, se necessário, seleccione as seguintes definições:

- Seleccione as definições do servidor de proxy que serão utilizadas durante a actualização:

  Detectar automaticamente as definições do servidor de proxy. Se seleccionar esta opção, as definições de proxy são detectadas automaticamente através do protocolo WPAD (Web Proxy Auto-Discovery Protocol). Se este protocolo não conseguir detectar o

endereço, o Kaspersky Anti-virus usará as definições do servidor de proxy especificadas no Microsoft Internet Explorer.

Utilizar definições personalizadas do servidor de proxy – utilize um proxy diferente do especificado nas definições de ligação do navegador. No campo **Endereço**, introduza ou o endereço IP ou o nome simbólico do servidor de proxy e no campo **Porta** especifique o número da porta de proxy.

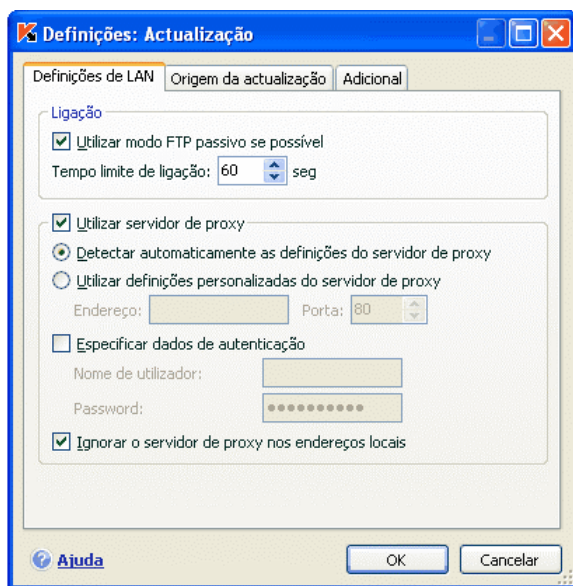



Figura 71. Configurar definições de actualização da rede

- Especifique se é necessária autenticação no servidor de proxy. *Autenticação* é o processo de verificação dos dados de registo do utilizador para fins de controlo de acesso.

  Se for necessária autenticação para ligar ao servidor de proxy, assinale a opção **Especificar dados de autenticação** e especifique o nome de utilizador e password nos campos que surgem em baixo. Nesse caso, primeiro tenta-se a autenticação por NTLM e depois a autenticação por BASIC.

  Se esta caixa não estiver seleccionada ou se os dados não forem inseridos, a autenticação por NTLM será tentada, utilizando a conta de utilizador usada para iniciar a actualização (ver 6.4 na pág. 87).

  Se o servidor de proxy requer autenticação e você não tiver introduzido o nome de utilizador e password ou, se por alguma razão, os dados

especificados não tiverem sido aceites pelo servidor de proxy, surgirá uma janela quando a actualização começar, pedido o nome de utilizador e password para autenticação. Se a autenticação for bem-sucedida, o nome de utilizador e password serão utilizados nas próximas actualizações. Caso contrário, as definições serão novamente solicitadas.

Para evitar utilizar uma proxy quando a origem de actualização é uma pasta local, seleccione a opção ☑ **Ignorar o servidor de proxy nos endereços locais**.

> Esta função não está disponível com o Windows 9X/NT 4.0. No entanto, por definição, o servidor de proxy não é utilizado para os endereços locais.

16.4.4. Distribuição de actualizações

A função de cópia de actualizações permite optimizar a carga na rede da sua empresa. As actualizações são copiadas em duas etapas:

1. Um dos computadores da rede recolhe um pacote de actualização da aplicação e das assinaturas de ameaças a partir dos servidores da Kaspersky Lab ou a partir de outro recurso da Internet que aloja um conjunto de actualizações correntes. As actualizações recolhidas são colocadas numa pasta de acesso público.
2. Os outros computadores da rede acedem à pasta de acesso público para recolher as actualizações da aplicação.

Para activar a distribuição de actualizações, seleccione a caixa ☑ **Pasta de distribuição de actualizações** no separador **Adicional** (ver Figura 72) e no campo em baixo especifique a pasta partilhada onde serão colocadas as actualizações recolhidas. Pode inserir um caminho manualmente ou seleccioná-lo na janela que se abre quando clica em **Procurar**. Se a caixa for seleccionada, as actualizações serão automaticamente copiadas para esta pasta quando forem recolhidas.

> Note que o Kaspersky Anti-virus 6.0 apenas recolhe pacotes de instalação para as aplicações da versão 6.0 a partir dos servidores de actualização da Kaspersky Lab. Recomendamos que copie as actualizações para outras aplicações da Kaspersky Lab através do Kaspersky Administration Kit.

Se quiser que outros computadores da rede actualizem a partir da pasta que contém as actualizações copiadas da Internet, tem que seguir os seguintes passos:

1. Conceder acesso público a esta pasta.

2. Especificar a pasta partilhada como a origem da actualização nos computadores da rede, nas definições do Actualizador.

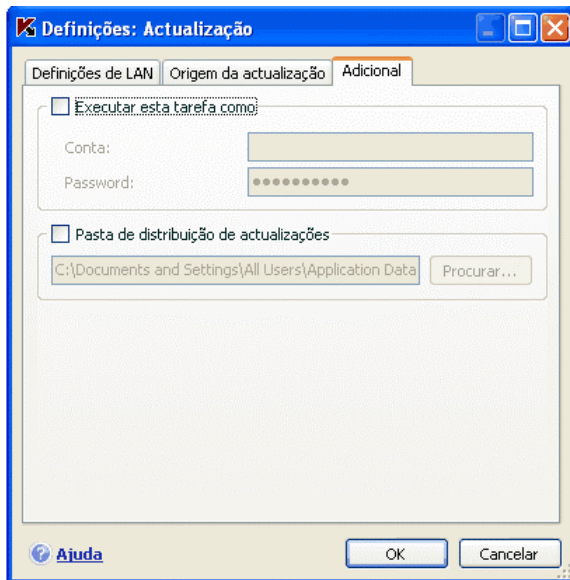



Figura 72. Definições da ferramenta de cópia de actualizações

16.4.5. Acções depois de actualizar o programa

Cada actualização de assinaturas de ameaças contém registos novos que protegem o seu computador das últimas ameaças.

A Kaspersky Lab recomenda a verificação dos ficheiros em quarentena e dos objectos de inicialização sempre que a base de dados for actualizada.

Porque é que estes ficheiros devem ser analisados?

A quarentena contém ficheiros que foram marcados pelo programa como suspeitos ou possivelmente infectados (ver 17.1 na pág. 239). Utilizando a última versão das assinaturas de ameaças, o Kaspersky Anti-virus para Windows Workstations poderá identificar a ameaça e eliminá-la.

Por definição, a aplicação analisa os ficheiros em quarentena depois de cada actualização das assinaturas de ameaças. Também recomendamos que examine, periodicamente, os ficheiros em quarentena porque o seu estado pode

alterar-se após várias verificações. Alguns ficheiros podem então ser restaurados às localizações prévias e poderá continuar a trabalhar com eles.

Para desactivar a verificação dos ficheiros em quarentena, desmarque a opção ☑ **Verificar novamente a Quarentena** na secção **Acção após Actualização**.

Os objectos de inicialização são críticos para a segurança do seu computador. Se um deles estiver infectado com uma aplicação maliciosa, isto pode levar a uma falha na inicialização do sistema operativo. O Kaspersky Anti-virus para Windows Workstations possui uma tarefa de verificação incorporada para os objectos de inicialização (ver Capítulo 14 na pág. 204). Recomendamos que estabeleça um agendamento para esta tarefa de forma a que seja automaticamente iniciada após cada actualização das assinaturas de ameaças (ver 6.5 na pág. 88).

CAPÍTULO 17. OPÇÕES AVANÇADAS

O Kaspersky Anti-Virus para Windows Workstations possui outras características que aumentam a sua funcionalidade.

O programa coloca alguns ficheiros em áreas de armazenamento especiais. Isto assegura a protecção máxima dos dados com perdas mínimas.

- A cópia de segurança contém cópias de ficheiros que o Kaspersky Anti-Virus para Windows Workstations alterou ou apagou (ver 17.2 na pág. 243). Se algum ficheiro continha informação que era importante para si e que não pôde ser totalmente recuperada durante o processamento do anti-vírus, pode sempre restaurar o ficheiro a partir desta cópia de segurança.
- A quarentena contém ficheiros, potencialmente, infectados que não puderam ser processados utilizando as actuais assinaturas de ameaças (ver 17.1 na pág. 239).

Recomenda-se que examine, periodicamente, a lista de ficheiros. Alguns deles podem já estar desactualizados e alguns podem ter sido restaurados.

Algumas das características foram concebidas para o ajudar enquanto utiliza o programa. Por exemplo:

- O Suporte Técnico fornece assistência polivalente com o Kaspersky Anti-virus para Windows Workstations (ver 17.6 na pág. 266). A Kaspersky Lab fornece-lhe todos os meios de apoio possíveis: apoio on-line, um fórum de perguntas e respostas para os utilizadores do programa, etc.
- A funcionalidade Notificações disponibiliza ao utilizador notificações sobre momentos-chave no Kaspersky Anti-virus para Windows Workstations (ver 17.11.1 na pág. 278). Podem ser eventos com natureza informativa ou erros que devem ser imediatamente eliminados e sobre os quais é necessário ter conhecimento.
- A Autodefesa protege os ficheiros do próprio programa de serem modificados ou danificados por hackers, bloqueia a administração remota da utilização das funcionalidades do programa e restringe a possibilidade de outros utilizadores no seu computador de efectuarem certas acções no Kaspersky Anti-virus para Windows Workstations (ver 17.11.1.2 na pág. 280). Por exemplo, alterar o nível de protecção pode influenciar, significativamente, a segurança da informação no seu computador.

- O Gestor da Chave de Licença pode obter informação detalhada sobre a licença utilizada, activar a sua cópia do programa e gerir ficheiros de chaves de licença (ver 17.5 na pág. 264).

O programa também fornece uma secção de Ajuda (ver 17.4 na pág. 263) e relatórios detalhados (ver 17.3 na pág. 245) sobre o funcionamento de todas as componentes de protecção, actualizações e tarefas de verificação de vírus.

A criação de uma lista de portas monitorizadas pode regular que módulos do Kaspersky Anti-virus para Windows Workstations controlam os dados transferidos nas portas seleccionadas (ver 17.7 na pág. 267).

O Disco de Recuperação permite restaurar a funcionalidade do seu computador depois de uma infecção (ver 17.10 na pág. 273). Isto é particularmente útil quando não consegue carregar o sistema operativo do seu computador depois de um código malicioso ter danificado ficheiros do sistema.

Você também pode alterar o aspecto do Kaspersky Anti-virus para Windows Workstations e pode personalizar a interface do programa (ver 17.9 na pág. 271).

As secções que se seguem irão discutir, em detalhe, estas funções.

17.1. Quarentena para objectos potencialmente infectados

A **Quarentena** é uma área de armazenamento especial que contém ficheiros, potencialmente, infectados com vírus.

Os **objectos, potencialmente, infectados** são ficheiros que se suspeita estarem infectados com vírus ou modificações de vírus.

Porquê *potencialmente infectados*? Nem sempre é possível determinar se um ficheiro está infectado. Isto pode acontecer por várias razões:

- O código do ficheiro analisado é parecido com uma ameaça conhecida mas está parcialmente modificado.

  As assinaturas de ameaças contêm ameaças que já foram estudadas pela Kaspersky Lab. Se um programa malicioso é modificado e estas alterações ainda não foram introduzidas nas assinaturas, o Kaspersky Anti-virus para Windows Workstations classifica o objecto infectado com o programa malicioso alterado como um ficheiro, potencialmente, infectado e indicará a ameaça com a qual esta infecção se assemelha.

- O código do ficheiro detectado faz lembrar a estrutura de uma sequência de vírus de um programa malicioso. No entanto, não existe nada similar nas assinaturas de ameaça.

  É possível que seja um novo tipo de ameaça, por isso o Kaspersky Anti-virus para Windows Workstations classifica o ficheiro como um ficheiro, potencialmente, infectado.

O analisador do código *heurístico* detecta vírus potenciais. O mecanismo é bastante eficaz e muito raramente produz falsos diagnósticos positivos.

Um ficheiro potencialmente infectado pode ser detectado e colocado em quarentena pelo Anti-vírus de Ficheiros, Anti-vírus de E-mail, Defesa Pró-activa ou durante uma verificação de vírus.

Pode colocar um ficheiro em quarentena clicando em **Quarentena** na notificação que aparece quando é detectado um ficheiro potencialmente infectado.

Quando coloca um ficheiro em Quarentena, este é movido e não copiado. O ficheiro é apagado do disco ou do e-mail e é guardado na pasta Quarentena. Os ficheiros em Quarentena são guardados num formato especial e não são perigosos.

17.1.1. Acções com ficheiros em quarentena

O número total de ficheiros em **Quarentena** é exibido na secção **Ficheiros de Dados** do **Serviço**. Na parte direita do ecrã, a secção *Quarentena* mostra:

- o número de ficheiros potencialmente infectados detectados durante o funcionamento do Kaspersky Anti-virus para Windows Workstations;
- o tamanho actual da Quarentena.

Aqui pode apagar todos os ficheiros em quarentena com o botão **Limpar**. Note que ao fazer isso os ficheiros de da cópia de segurança e ficheiros de relatórios também serão apagados.

Para aceder aos objectos em Quarentena:

Clique com o botão esquerdo do rato na secção **Quarentena**.

Pode efectuar as seguintes acções no Separador **Quarentena** (ver Figura 73):

- Move a file to Quarantine that you suspect is infected but the program did not detect. To do so, click **Add** and select the file in the standard selection window. It will be added to the list with the status *added by user*.

- Mover para a **Quarentena** um ficheiro que você suspeita estar infectado, mas que o programa não detectou. Para o fazer, clique em **Adicionar** e seleccione o ficheiro de que necessita na janela de selecção. Será adicionado à lista com o estado *adicionado pelo utilizador*.

> Se colocou, manualmente, um ficheiro na quarentena e se, depois de uma verificação subsequente, se conclui que o objecto não está infectado, o seu estado após a verificação não, será automaticamente, alterado para *OK*. Isto apenas acontecerá se a verificação ocorrer decorrido um certo tempo (pelo menos, três dias) após a sua colocação na quarentena.

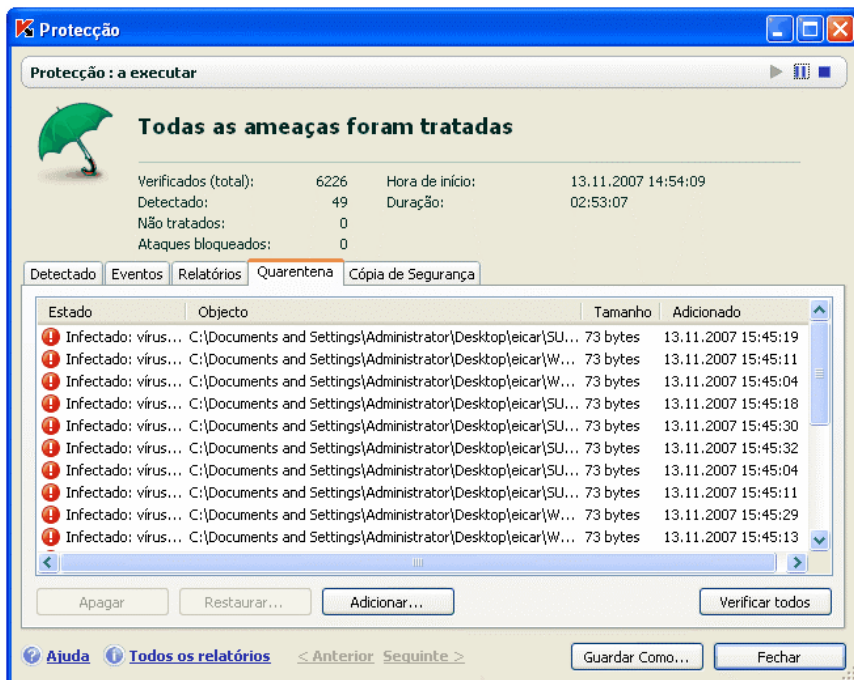



Figura 73. Lista de objectos em quarentena

- Analisar e desinfectar todos os objectos potencialmente infectados na Quarentena utilizando as assinaturas de ameaças actuais. Para o fazer, clique em **Verificar todos**.

  Depois de analisar e desinfectar qualquer objecto em quarentena, o seu estado poderá alterar-se para *infectado, potencialmente infectado, falso diagnóstico positivo, OK*, etc.

O estado *infectado* significa que o objecto foi identificado como infectado mas não pôde ser tratado. Recomendamos que apague esses objectos.

Todos os objectos marcados como *falsos diagnósticos positivos* podem ser restaurados, já que o seu estado anterior de *potencialmente infectados* não foi confirmado pelo programa ao ser novamente analisado.

- Restaurar os ficheiros para uma pasta seleccionada ou para a sua pasta original anterior à Quarentena (opção predefinida). Para restaurar um ficheiro, seleccione-o de uma lista e clique em **Restaurar**. Quando restaurar ficheiros a partir de arquivos, bases de dados de e-mails e ficheiros com formato de e-mail colocados na Quarentena, também deverá seleccionar o directório para o qual os restaura.

> Dica:
>
> Recomendamos que só restaure os objectos com o estado *falso diagnóstico positivo, OK, desinfectado*, já que ao restaurar outros ficheiros pode levar à infecção do seu computador.

- Apagar qualquer objecto ou grupo de objectos seleccionados em quarentena. Apenas apague ficheiros que não possam ser desinfectados. Para apagar ficheiros, seleccione-os na lista e clique em **Apagar**.

17.1.2. Configurar a Quarentena

Pode definir as definições para o esquema de funcionamento da Quarentena, especificamente:

- Configurar verificações automáticas para os ficheiros em Quarentena depois de cada actualização das assinaturas de ameaças (para mais detalhes, ver 16.4.4 na pág. 235).

> Aviso!
>
> Se estiver a utilizar a Quarentena, o programa não poderá verificar ficheiros em quarentena, imediatamente, a seguir à actualização das assinaturas de ameaças.

- Estabelecer o tempo máximo de armazenamento na Quarentena.

  O tempo de armazenamento predefinido é de 30 dias, ao fim do qual os ficheiros são apagados. Você pode alterar o tempo de armazenamento da Quarentena ou desactivar esta restrição.

Para o fazer:

1. Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Na secção **Quarentena e Cópia de Segurança** (ver Figura 74), introduza o período de tempo após o qual os ficheiros em Quarentena serão automaticamente apagados. Em alternativa, desmarque a caixa para desactivar a eliminação automática.

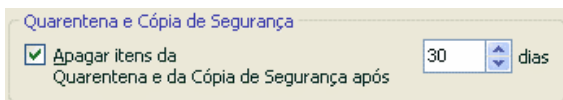



Figura 74. Configurar o período de armazenamento em Quarentena

17.2. Cópias de segurança de objectos perigosos

Algumas vezes, quando os ficheiros são desinfectados, a sua integridade perde-se. Se um ficheiro desinfectado contém informação importante e se depois da desinfecção essa informação é parcial ou completamente corrompida, pode tentar restaurá-lo a partir de uma cópia de segurança.

Uma cópia de segurança é uma cópia do ficheiro perigoso original que é criada quando o ficheiro é primeiro desinfectado ou apagado. É guardado na **Cópia de Segurança**.

A **Cópia de Segurança** é uma área de armazenamento especial que contém as cópias de segurança de ficheiros perigosos. Os ficheiros são guardados na Cópia de Segurança com um formato especial e não são perigosos.

17.2.1. Acções com cópias de segurança

O número total de cópias de segurança de ficheiros na Cópia de Segurança é exibido nos **Ficheiros de Dados** na secção **Serviço**. Na parte direita do ecrã existe uma caixa especial *Cópia de Segurança* que exibe:

- o número de cópias de segurança de ficheiros criadas pelo Kaspersky Anti-Virus para Windows Workstations.
- o tamanho actual da Cópia de Segurança.

Aqui pode apagar todas as cópias armazenadas em Cópias de Segurança com o botão **Limpar**. Note que ao fazer isto, os ficheiros em Quarentena e os ficheiros de relatórios também serão apagados.

Para aceder à cópia de ficheiros perigosos:

> Clique com o botão esquerdo do rato em qualquer parte da secção **Cópia de Segurança**.

Uma lista das cópias de segurança é exibida no Separador Cópia de Segurança (ver Figura 75). A seguinte informação é exibida para cada cópia: nome completo do ficheiro com o atalho para a localização original, estado do ficheiro atribuído pela verificação e o seu tamanho.

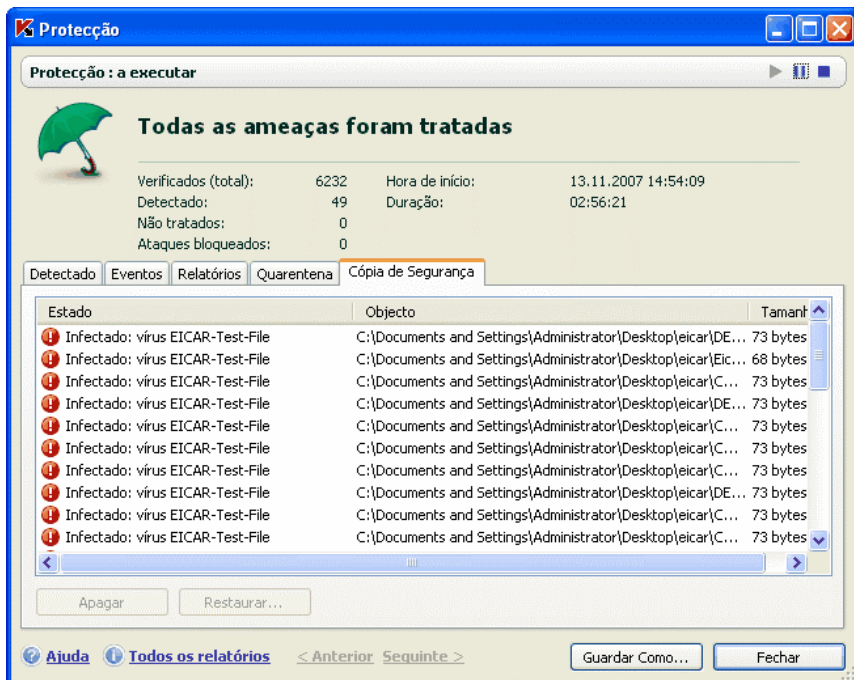



Figura 75. Lista de objectos da cópia de segurança

Pode restaurar as cópias seleccionadas utilizando o botão **Restaurar**. O ficheiro é restaurado a partir de uma Cópia de Segurança, mantendo o mesmo nome que possuía antes da desinfecção.

Se já há um ficheiro na localização original com esse nome (é possível, se foi feita uma cópia do ficheiro a ser restaurado antes da desinfecção), surgirá o

aviso correspondente. Pode alterar a localização do ficheiro restaurado ou dar-lhe um novo nome.

Recomendamos a verificação do ficheiro, imediatamente, a seguir a restaurá-lo. É possível que com as assinaturas actualizadas, você possa desinfectá-lo sem perder a integridade do ficheiro.

Desaconselhamos o restaurar de cópias de segurança de ficheiros, a menos que seja absolutamente necessário. Isto pode levar a uma infecção no seu computador.

Recomendamos que examine, periodicamente, a Cópia de Segurança e a esvazie utilizando o botão **Apagar**. Também pode configurar o programa para que ele apague, automaticamente, as cópias de Segurança mais antigas (ver 17.2.2 na pág. 245).

17.2.2. Configurar as definições de Cópia de Segurança

Pode definir o tempo máximo de armazenamento na Cópia de Segurança.

O tempo de armazenamento predefinido da Cópia de Segurança é de 30 dias, ao fim do qual os ficheiros são apagados. Você pode alterar este tempo de armazenamento ou desactivar esta restrição. Para o fazer:

1. Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Na secção **Quarentena e Cópia de Segurança** (ver Figura 74) estabeleça a duração para o armazenamento das cópias de segurança, na parte direita do ecrã. Em alternativa, desmarque a caixa para desactivar a eliminação automática.

17.3. Relatórios

As acções das componentes, das tarefas de verificação de vírus e de actualizações do Kaspersky Anti-virus para Windows Workstations são guardadas num relatório.

O número total de relatórios criados pelo programa e o seu tamanho total é exibido nos **Ficheiros de Dados** na secção **Serviço** na janela principal do Programa. Esta informação é exibida na caixa.

Para visualizar os relatórios:

> Clique com o botão esquerdo do rato na caixa *Relatórios* para abrir a janela Protecção, que resume a protecção fornecida pela aplicação. Uma janela abrir-se-á para o separador **Relatórios** (ver Figura 76).

O separador Relatórios lista os últimos relatórios sobre todas as componentes e tarefas de verificação de vírus e de actualização que se efectuaram durante a actual sessão do Kaspersky Anti-virus para Windows Workstations. A informação é exibida acerca de todas as componentes e tarefas. Por exemplo, parado ou completo. Se deseja visualizar o histórico completo da criação de relatórios para a actual sessão do programa, seleccione **Mostrar histórico de relatórios**.

Para rever todos os eventos gravados no relatório de uma componente ou tarefa:

> Seleccione o nome da componente ou tarefa no Separador **Relatórios** e clique no botão **Detalhes**.

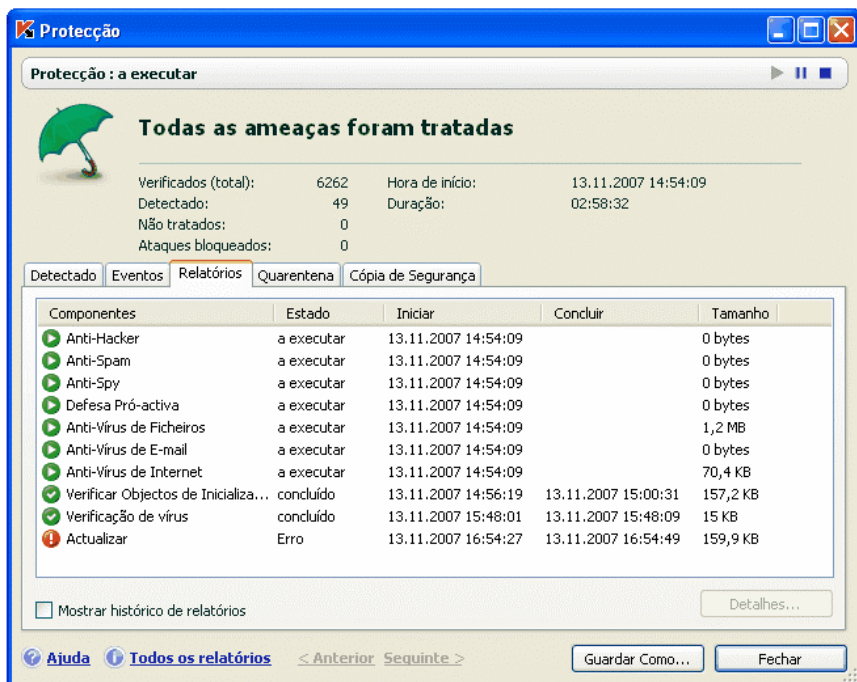



Figura 76. Relatórios sobre o funcionamento de componentes

Abrir-se-á uma janela com informação detalhada sobre o desempenho da componente ou tarefa seleccionada. As estatísticas de desempenho resultantes são exibidas na parte superior da janela e é fornecida informação detalhada nos Separadores. Dependendo da componente ou da tarefa, os Separadores podem variar:

- O Separador **Detectado** contém uma lista dos ficheiros perigosos detectados por uma componente ou por uma tarefa de verificação de vírus.
- O Separador **Eventos** exibe os eventos de componentes ou tarefas.
- O Separador **Estatísticas** contém estatísticas detalhadas para todos os ficheiros analisados.
- O Separador **Definições** mostra as definições utilizadas pelas componentes de protecção, verificações de vírus ou actualizações de assinaturas de ameaças.
- Os Separadores **Macros** e **Registo** só existem no relatório da **Defesa Pró-activa** e contêm informação sobre todas as macros que tentaram executar-se no seu computador e sobre todas as tentativas para modificar o registo do sistema operativo.
- Os Separadores **Phishing**, **Popups**, **Banners** e as **Ligações Telefónicas** só poderão ser encontrados no relatório do Anti-Spy. Eles incluem informação sobre todos os ataques de phishing detectados e todas as janelas de popups, banners e tentativas de ligações telefónicas bloqueadas durante aquela sessão do programa.
- Os separadores **Ataques de rede**, **Anfitriões Banidos**, **Actividade da aplicação** e **Filtragem de Pacotes** só poderão ser encontrados no relatório do Anti-Hacker. Eles incluem informação sobre todas as tentativas de ataques de rede no seu computador, anfitriões banidos depois de ataques, descrições da actividade de rede das aplicações que condiz com as regras de actividade existentes e todos os pacotes de dados que condizem com as regras de filtragem de pacotes da Anti-Hacker.
- Os Separadores **Ligações estabelecidas, Portas abertas** e **Tráfego** também cobrem a actividade de rede do seu computador, exibindo as ligações actualmente estabelecidas, portas abertas e a quantidade de tráfego de rede que o seu computador enviou e recebeu.

Pode exportar todo o relatório como um ficheiro de texto. Esta característica é útil nos casos onde ocorreu um erro numa componente ou tarefa que você não pode eliminar sozinho e precisa da ajuda do Suporte Técnico. Se isto acontecer, o relatório deve ser enviado em formato .txt para o Suporte Técnico para que os

nossos especialistas possam estudar o problema detalhadamente e resolvê-lo o mais rapidamente possível.

Para exportar um relatório como um ficheiro de texto:

Clique em **Guardar como** e especifique onde deseja guardar o ficheiro de relatório.

Quando acabar de trabalhar com o relatório, clique em **Fechar**.

Existe um botão **Acções** em todos os Separadores (excepto no separador Definições e Estatísticas) e que pode utilizar para definir respostas aos objectos na lista. Quando clica nele, abre-se um menu de contexto com os seguintes itens de menu (dependendo da componente, o menu difere – todas as opções possíveis estão listadas em baixo):

Desinfectar – tenta desinfectar um objecto perigoso. Se o objecto não for desinfectado com sucesso, pode deixá-lo nesta lista para o analisar mais tarde com assinaturas de ameaças actualizadas ou apagá-lo. Pode aplicar esta acção a um único objecto da lista ou a vários objectos.

Apagar – apaga o registo da detecção do objecto da lista.

Adicionar à Zona Confiável – exclui o objecto da protecção. Uma janela abrir-se-á com uma regra de exclusão para o objecto.

Ir para o Ficheiro – abre a pasta onde se encontra o objecto no Windows Explorer.

Neutralizar todos – neutraliza todos os objectos da lista. O Kaspersky Anti-virus para Windows Workstations tentará processar os objectos, utilizando as assinaturas de ameaças.

Descartar todos – esvazia o relatório dos objectos detectados. Ao utilizar esta função, todos os objectos perigosos detectados permanecem no seu computador.

Ver em http://www.viruslist.com/ – vai para uma descrição do objecto na Enciclopédia de Vírus da Kaspersky Lab.

Ver em www.google.com – encontra informação acerca do objecto, utilizando este motor de busca.

Procurar – introduz termos de pesquisa (por nome ou estado) para os objectos existentes na lista.

Além disso, pode ordenar a informação exibida na janela por ordem ascendente e descendente para cada uma das colunas, clicando no cabeçalho da coluna.

17.3.1. Configurar as definições dos relatórios

Para configurar definições para criar e guardar relatórios:

1. Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations clicando em Definições na janela principal do programa.
2. Seleccione **Ficheiros de Dados** na árvore de definições.
3. Edite as definições na caixa **Relatórios** (ver Figura 77) como se segue:
    - Active ou desactive o registo de eventos informativos. Normalmente, estes eventos não são importantes para a segurança. Para registar eventos, seleccione ☑ **Registar eventos não críticos**;
    - Escolha apenas guardar eventos no relatório que ocorreram desde a última vez que a tarefa foi realizada. Isto poupa espaço no disco ao reduzir no tamanho do relatório. Se for seleccionada a opção ☑ **Guardar apenas eventos recentes**, a informação no relatório será actualizada todas as vezes que reiniciar a tarefa. No entanto, só a informação não crítica será apagada.
    - Configure o tempo de armazenamento para relatórios. Por definição, o tempo de armazenamento dos relatórios é de 30 dias, ao fim dos quais os relatórios serão apagados. Pode alterar o tempo máximo de armazenamento ou remover esta restrição.

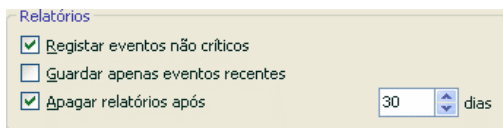



Figura 77. Configurar definições do relatório

17.3.2. Separador *Detectadas*

Este Separador (ver Figura 78) contém uma lista dos ficheiros perigosos detectados pelo Kaspersky Anti-virus para Windows Workstations. É indicado o

nome completo para cada ficheiro, juntamente com o estado atribuído pelo programa quando ele foi analisado e processado.

Se deseja que a lista contenha tanto os ficheiros perigosos, como os ficheiros neutralizados com sucesso, seleccione **Mostrar objectos neutralizados**.

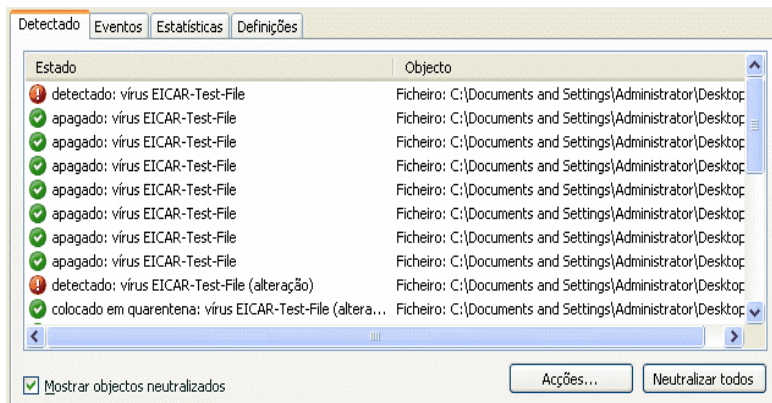



Figura 78. Lista dos objectos perigosos detectados

Para processar objectos perigosos detectados pelo Kaspersky Anti-Virus, clique no botão **Desinfectar** (para um objecto ou um grupo de objectos seleccionados) ou **Neutralizar todos** (para processar todos os objectos na lista). Quando cada objecto for processado, aparecerá uma mensagem no ecrã. Aqui terá que decidir o que fazer com os mesmos a seguir.

Se assinalar a opção **Aplicar a todos os casos semelhantes** na janela de notificação, a acção seleccionada será aplicada a todos os objectos com o estado seleccionado na lista antes de ter começado o processamento.

17.3.3. Separador *Eventos*

Este Separador (ver Figura 79) fornece-lhe uma lista completa de todos os eventos importantes no funcionamento da componente de protecção, verificações de vírus e actualizações das assinaturas de ameaças e que não foram ignorados por uma regra de controlo de actividade (ver 10.1.1 na pág. 131).

Eventos críticos – são eventos de importância crítica que apontam para problemas no funcionamento do programa ou vulnerabilidades no seu computador. Por exemplo, *vírus detectado, erro na operação*.

Eventos importantes – são eventos que devem ser investigados, já que eles reflectem situações importantes no funcionamento do programa. Por exemplo, *parado.*

Mensagens informativas – são mensagens de referência tipo que geralmente não contêm informação importante. Por exemplo, *OK, não processado*. Estes eventos só se reflectem no registo de eventos se for seleccionada a opção **Mostrar todos os eventos**.

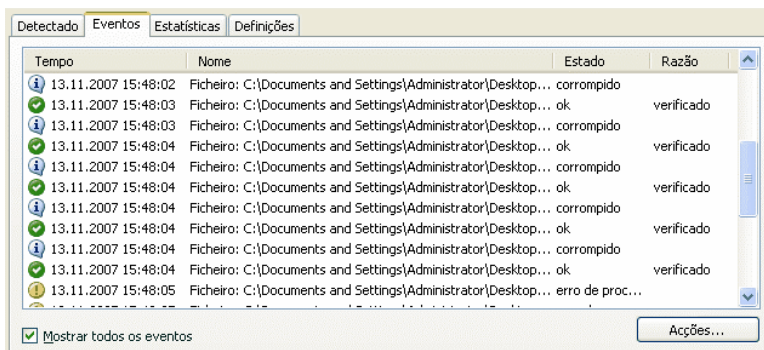



Figura 79. Eventos que ocorrem no funcionamento da componente

O formato de exibição de eventos no registo de eventos pode variar em função da componente ou tarefa. É dada a seguinte informação para as tarefas de actualização:

- Nome do evento
- Nome do ficheiro envolvido no evento
- Hora a que o evento ocorreu
- Tamanho do ficheiro transferido

Para as tarefas de verificação de vírus, o registo do evento contém o nome do ficheiro analisado e o estado que lhe foi atribuído pela verificação/processamento.

Pode também treinar o Anti-Spam enquanto visualiza o relatório, utilizando o menu de contexto especial. Para o fazer, seleccione o nome da mensagem de e-mail e abra o menu de contexto, clicando com o botão direito do rato e seleccionando **Marcar como Spam**, se o e-mail for spam, ou **Marcar como não-spam**, se o e-mail seleccionado for em e-mail bom. Além disso, com base na informação obtida ao analisar o e-mail, pode adicioná-lo às listas branca e negra do Anti-Spam. Para o fazer, utilize os itens correspondentes no menu de contexto.

17.3.4. Separador *Estatísticas*

Este Separador (ver Figura 80) fornece-lhe estatísticas detalhadas sobre as componentes e as tarefas de verificação de vírus. Aqui pode saber:

- Quantos ficheiros foram verificados nesta sessão de uma componente ou depois de uma tarefa estar terminada. É exibido o número de arquivos analisados, ficheiros comprimidos, objectos protegidos por password e objectos corrompidos.
- Quantos ficheiros perigosos foram detectados, não desinfectados, apagados e colocados em Quarentena.

Figura 80. Estatísticas da componente

17.3.5. Separador *Definições*

O Separador **Definições** (ver Figura 81) dá uma visão completa das definições das componentes de protecção, verificações de vírus e actualizações do programa. Pode descobrir o actual nível de segurança de uma componente ou uma verificação de vírus, que acções estão a ser efectuadas com os ficheiros perigosos ou que definições estão a ser utilizadas para as actualizações do programa. Utilize a ligação Alterar definições para configurar a componente.

Pode configurar as definições avançadas para as verificações de vírus:

- Estabeleça a prioridade das tarefas de verificação utilizadas se o processador estiver muito pesado. Por defeito, a opção ☑ **Conceder recursos para outras aplicações** não está seleccionada. Com esta funcionalidade, o programa verifica a carga do processador e dos subsistemas do disco para a actividade de outras aplicações. Se a carga no processador aumentar significativamente e impedir as aplicações do utilizador de funcionarem normalmente, o programa

reduzirá a actividade de verificação. Isto aumentará o tempo de verificação e libertará os recursos para as aplicações do utilizador.

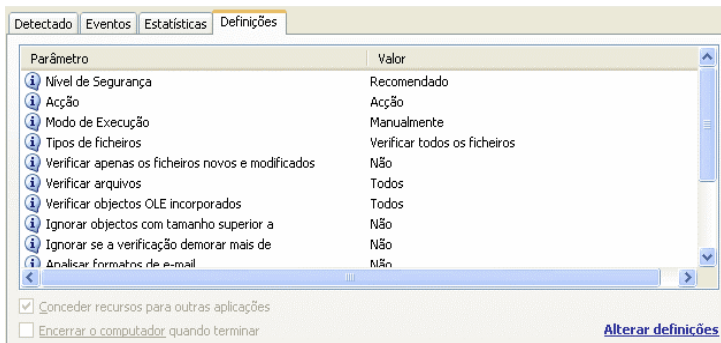



Figura 81. Definições da componente

- Configure o modo de funcionamento a executar depois da verificação de vírus estar completa. Pode configurar o computador para se desligar, reiniciar ou entrar em modo de espera ou de economia de energia. Para seleccionar uma opção, clique com o botão esquerdo do rato na ligação até que esta mostre a opção que deseja.

Pode precisar desta funcionalidade se, por exemplo, iniciar uma verificação de vírus no final de um dia de trabalho e não deseja esperar pelo seu fim.

Contudo, esta funcionalidade requer alguns passos adicionais: antes de iniciar a verificação, deve desactivar os pedidos de password para os objectos a serem verificados, se estiverem activados, e activar o processamento automático de objectos perigosos. Assim, as funcionalidades interactivas do programa serão desactivadas.

17.3.6. Separador *Macros*

Todas as macros que tentaram executar-se durante a sessão actual do Kaspersky Anti-virus para Windows Workstations estão listadas no Separador **Macros** (ver Figura 82). Aqui encontrará o nome completo de cada macro, a hora em que foi executada e o seu estado depois do processamento da macro.

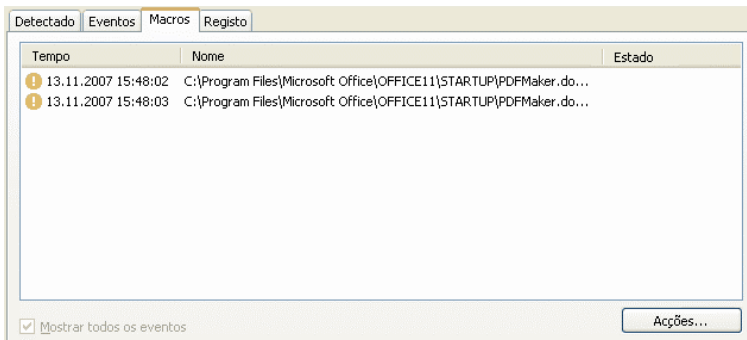



Figura 82. Macros perigosas detectadas

Pode escolher o modo de visualização para este separador, Se não deseja ver eventos informativos desmarque a opção ☑ **Mostrar todos os eventos**.

17.3.7. Separador *Registo*

No Separador **Registo** (ver Figura 83) o programa grava operações com chaves de registo que foram tentadas desde que o programa foi iniciado, a menos que tenham sido proibidas por uma regra (ver 10.1.3.2 na pág. 140).

O Separador lista o nome completo da chave, o seu valor, o tipo de dados e a informação sobre a operação que ocorreu: que acção foi tentada, a que horas e se foi permitida.

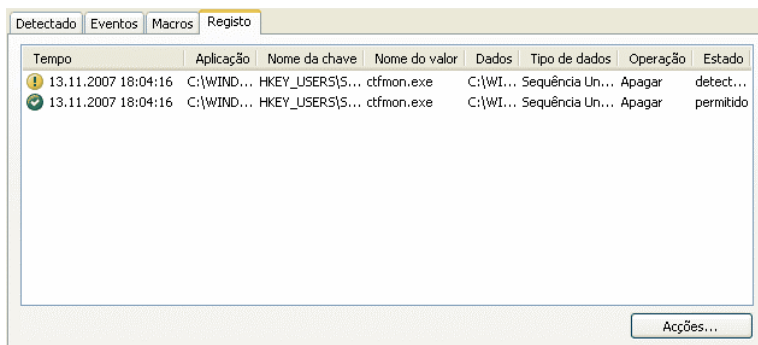



Figura 83. Ler e modificar eventos de registo de sistema

17.3.8. Separador *Phishing*

Este Separador de relatório (ver Figura 84) mostra todas as tentativas de phishing efectuadas durante a actual sessão do Kaspersky Anti-Virus para Windows Workstations. O relatório apresenta um link para o site phishing detectado no e-mail (ou noutra origem), a data e hora em que o ataque foi detectado e o estado do ataque (se foi bloqueado).

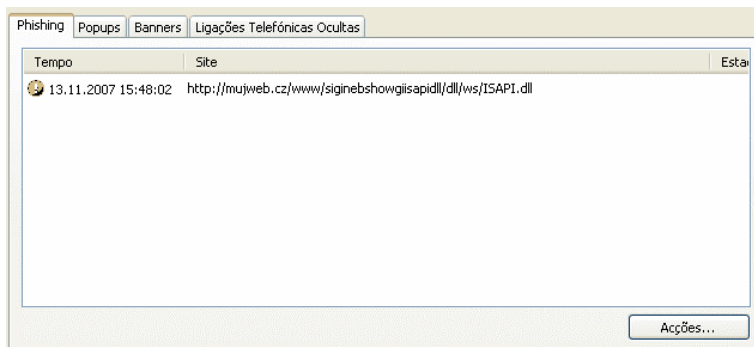



Figura 84. Ataques phishing bloqueados

17.3.9. Separador *Popups*

Este Separador de relatório (ver Figura 85) lista os endereços de todas as janelas de pop-up que o Anti-Spy bloqueou. Normalmente, estas janelas são abertas a partir de sites.

Para cada pop-up são gravados o endereço, a data e a hora em que o Bloqueador de Popups bloqueou a janela.

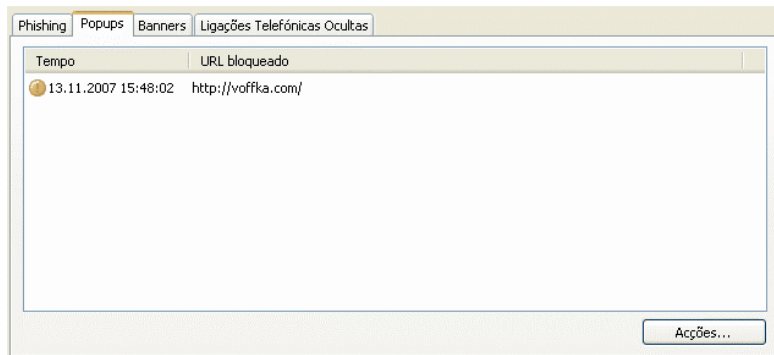



Figura 85. Lista de janelas popup bloqueadas

17.3.10. Separador *Banners*

Este Separador de relatório (ver Figura 86) contém os endereços dos banners que o Kaspersky Anti-Virus para Windows Workstations detectou na actual sessão. Para cada banner são listados os endereços de Internet, juntamente com o estado de processamento (banner bloqueado ou banner exibido).

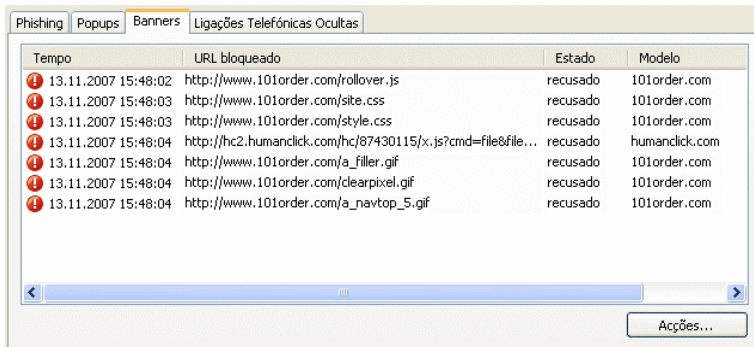



Figura 86. Lista de anúncios banner bloqueados

Você pode permitir que banners bloqueados sejam exibidos. Para o fazer, seleccione o objecto que pretende na lista e clique em **Acções** → **Permitir**.

17.3.11. Separador *Ligações Telefónicas Ocultas*

Este separador (ver Figura 87) apresenta todas as tentativas secretas para estabelecer ligações a sites pagos. Normalmente, essas tentativas são executadas por programas maliciosos instalados no seu computador.

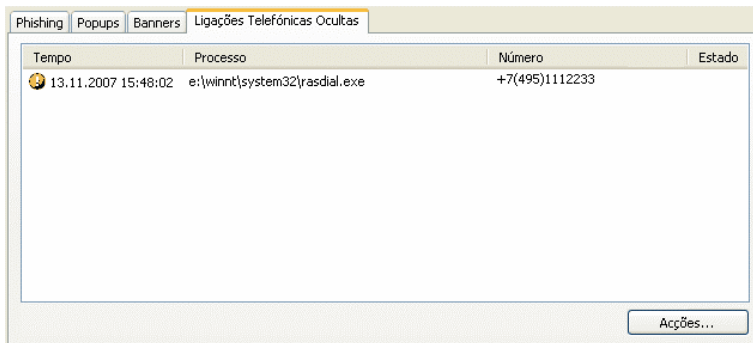



Figura 87. Lista de tentativas de ligações telefónicas

No relatório, você pode ver qual o programa que tentou ligar ao número de telefone para se ligar à Internet e o estado da tentativa: bloqueada ou permitida.

17.3.12. Separador *Ataques de rede*

Este separador (ver Figura 88) exibe um breve resumo dos ataques de rede no seu computador. Esta informação é guardada se o Sistema de Detecção de Intrusões estiver activado, o qual monitoriza todas as tentativas de ataque ao seu computador.

O Separador **Ataques de rede** lista a seguinte informação sobre os ataques:

- Fonte do ataque. Pode ser um endereço IP, anfitrião, etc.
- Porta local na qual ocorreu o ataque ao computador.
- Breve descrição do ataque.
- Hora a que o ataque ocorreu.

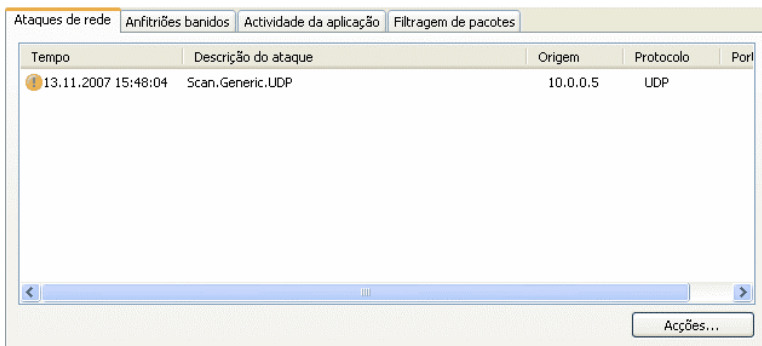



Figura 88. Lista de ataques na rede bloqueados

17.3.13. Separador *Anfitriões banidos*

Neste separador de relatório estão listados todos os anfitriões bloqueados a seguir a um ataque detectado pelo Sistema de Detecção de Intrusões (ver Figura 89).

É exibido o nome de cada anfitrião e a hora a que foi banido. Pode desbloquear um anfitrião neste Separador. Para o fazer, seleccione o anfitrião na lista e clique no botão **Acções** → **Desbloquear**.

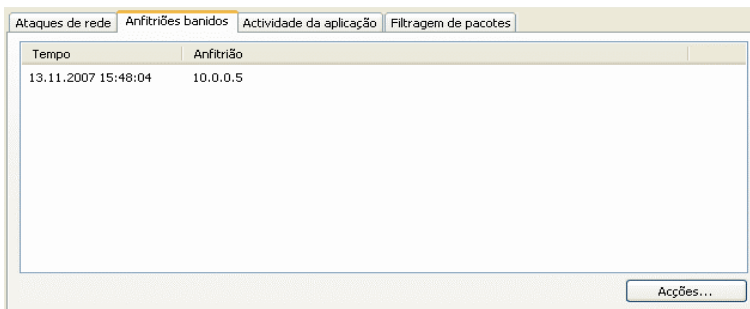



Figura 89. Lista de anfitriões bloqueados

17.3.14. Separador *Actividade da Aplicação*

No separador **Actividade da Aplicação** estão listadas todas as aplicações cujas actividades correspondam às regras de aplicações e que foram registadas pelo modulo *Firewall* durante a sessão actual do Anti-Hacker. (ver Figura 90).

A actividade só é gravada se estiver seleccionado a opção ☑ **Log de evento** na regra. Por defeito, esta opção está desmarcada nas regras de aplicações incluídas no Kaspersky Anti-Virus para Windows Workstations..

Este Separador exibe as propriedades básicas de cada aplicação (nome, PID, nome da regra) e um breve sumário da sua actividade (protocolo, direcção do pacote, etc.). Também é registada informação sobre se a actividade da aplicação é bloqueada.

Figura 90. Actividade da aplicação monitorizada

17.3.15. Separador *Filtragem de pacotes*

O Separador **Filtragem de pacotes** contém informação sobre o envio e recepção de pacotes que correspondem às regras de filtragem e que foram registados durante a actual sessão da aplicação (ver Figura 91).

Figura 91. Pacotes de dados monitorizados

A actividade só é gravada se estiver seleccionado a opção ☑ **Log de evento** na regra**.** Por defeito, esta opção está desmarcada nas regras de filtragem de pacotes incluídas no Kaspersky Anti-Virus para Windows Workstations.

Para cada pacote são indicados o resultado da filtragem (se o pacote foi bloqueado), a direcção do pacote, o protocolo e outras definições de ligação à rede para enviar e receber pacotes.

17.3.16. Separador *Ligações Estabelecidas*

Todas as ligações de rede activas, actualmente, estabelecidas no seu computador estão registadas no Separador **Ligações Estabelecidas** (ver Figura 92). Aqui encontrará o nome da aplicação que iniciou a ligação, o protocolo utilizado, a direcção da ligação (entrada ou saída), e as definições da ligação (portas e endereços IP locais e remotos). Também pode ver quanto tempo a ligação esteve activa e o volume de dados enviados ou recebidos. Pode criar ou apagar regras de ligação. Para o fazer, utilize as opções apropriadas no menu de contexto.

Aplicação	Linha de coma...	Protocolo	Direcção	Endereço local	Po
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
CCAPP.EXE		TCP	Entrada	127.0.0.1	10
CCAPP.EXE		TCP	Entrada	127.0.0.1	10
CCAPP.EXE		TCP	Entrada	127.0.0.1	10
CCAPP.EXE		TCP	Entrada	127.0.0.1	10
AVP.EXE	-R	TCP	Entrada	127.0.0.1	11
CCAPP.EXE		TCP	Saída	127.0.0.1	49

Figura 92. Lista de ligações estabelecidas

17.3.17. Separador *Portas Abertas*

No Separador *Portas abertas* (ver Figura 93) estão listadas todas as portas actualmente abertas no seu computador para as ligações de rede. Para cada porta, estão listados o número da porta, o protocolo de transferência de dados, o nome da aplicação que utiliza a porta e quanto tempo a porta esteve aberta.

Porta l...	Protocolo	Aplicação	Linha de coma...	Endereço local	Dura
445	UDP	System		0.0.0.0	03:23
445	TCP	System		0.0.0.0	03:23
138	UDP	System		172.16.2.7	03:23
137	UDP	System		172.16.2.7	03:23
139	TCP	System		172.16.2.7	03:23
135	TCP	SVCHOST.EXE	-K RPCSS	0.0.0.0	03:23
500	UDP	LSASS.EXE		0.0.0.0	03:23
4500	UDP	LSASS.EXE		0.0.0.0	03:23
1025	UDP	SVCHOST.EXE	-K NETWORKSER...	0.0.0.0	03:23
1026	UDP	SVCHOST.EXE	-K NETWORKSER...	0.0.0.0	03:23
123	UDP	SVCHOST.EXE	-K NETSVCS	172.16.2.7	03:23
123	UDP	SVCHOST.EXE	-K NETSVCS	127.0.0.1	03:23
1110	TCP	AVP.EXE	-R	127.0.0.1	03:23

Figura 93. Lista de portas abertas num computador

Esta informação poderá ser útil durante surtos de vírus e ataques de rede se você souber, exactamente, qual a porta vulnerável. Pode descobrir se aquela porta está aberta no seu computador e efectuar os procedimentos necessários para proteger o seu computador (por exemplo, activando o Sistema de Detecção de Intrusões, fechando a porta vulnerável ou criando uma regra para a mesma).

17.3.18. Separador *Tráfego*

Este Separador (ver Figura 94) contém informação sobre todas as ligações de entrada e de saída estabelecidas entre o seu computador e outros computadores, incluindo servidores de Internet, servidores de e-mail, etc. A seguinte informação é dada para cada ligação: nome e endereço IP do anfitrião com o qual é feita a ligação e a quantidade de tráfego enviada e recebida.

Anfitrião	Endereço IP	Rec...	Envi...
tl-2k-server2	172.16.6.62	74 bytes	0 bytes
ak-installtest.ak.ak20...	172.16.2.69	3,5 KB	0 bytes
ak_c225_2003	172.16.6.67	74 bytes	0 bytes
moscow3.avp.ru	91.103.64.3	22,5 KB	9,3 KB
moscow4.avp.ru	91.103.64.4	0 bytes	164 by...
nghtf-2.ak2003.avp.ru	172.16.1.73	310 by...	0 bytes
tl-oc17-w2k	172.16.6.95	3,0 KB	0 bytes
ak-171-2ksrv2.ak200...	172.16.4.100	742 by...	0 bytes
netserver.avp.ru	91.103.64.36	4,7 KB	2,5 KB
tlserver.avp.ru	172.16.10.100	3,2 KB	0 bytes
tl-2k3r2-s	172.16.4.116	2,5 KB	0 bytes
loginova.avp.ru	172.16.129.7	1,8 KB	0 bytes
172.16.10.128	172.16.10.128	74 bytes	0 bytes
ubuntu.avp.ru	172.16.4.134	978 by...	0 bytes
education.avp.ru	172.16.4.138	74 bytes	0 bytes
tl-vpsa	172.16.128.18	1,6 KB	0 bytes
10.64.0.7	10.64.0.7	21,6 MB	325,0 KB
lena-xp1	172.16.130.24	6,6 KB	8 KB
213-155-151-95.cust...	213.155.151.95	0 bytes	186 by...
213-155-151-97.cust...	213.155.151.97	0 bytes	186 by...
172.16.10.164	172.16.10.164	2,3 KB	0 bytes

Figura 94. Tráfego nas ligações de rede estabelecidas

17.4. Informação geral sobre o programa

Pode visualizar a informação geral sobre o programa na secção **Serviço** da janela principal (ver Figura 95).

Toda a informação está dividida em três secções:

- Na caixa **Informação sobre o Produto**, são exibidas as informações sobre a versão do programa, a data da última actualização e o número de ameaças conhecidas até à data.
- A informação básica sobre o sistema operativo instalado no seu computador está na caixa **Informação sobre o Sistema**.
- A informação básica sobre a licença que comprou para o Kaspersky Anti-virus está na caixa **Informação sobre a licença**.

Precisará de toda esta informação ao contactar o Suporte Técnico da Kaspersky Lab (ver 17.6 na pág. 266).

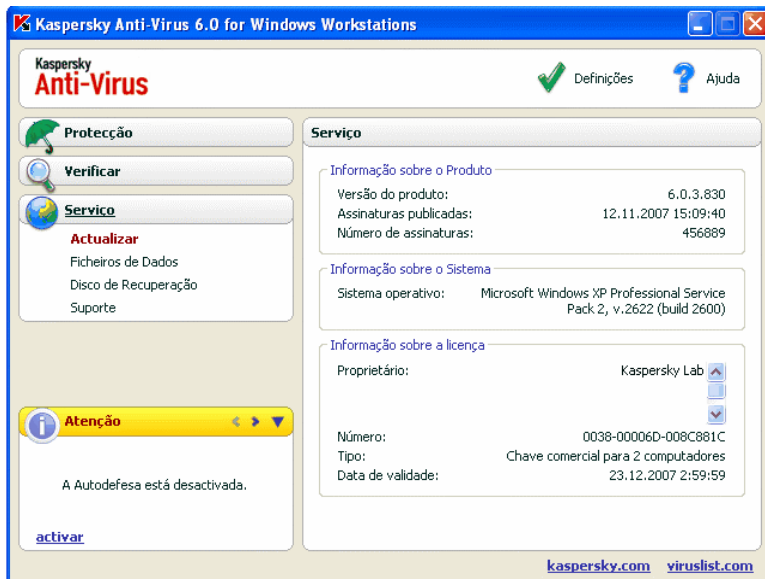



Figura 95. Informação sobre o programa, a licença e o sistema em que está instalado

17.5. Gerir licenças

O Kaspersky Anti-Virus para Windows Workstations precisa de uma *chave de licença* para funcionar. É-lhe fornecida uma chave quando adquirir o produto e dá-lhe o direito de utilizar o programa a partir do dia em que instala a chave.

Sem uma chave de licença, a não ser que tenha activado uma versão de avaliação da aplicação, o Kaspersky Anti-virus funcionará no modo de uma actualização. O programa não transferirá nenhuma actualização nova.

Se tiver activado uma versão de avaliação do programa, após terminar o período de avaliação, o Kaspersky Anti-vírus deixará de funcionar.

Quando uma chave de licença comercial expira, o programa continua a trabalhar, mas não poderá fazer as actualizações das assinaturas de ameaças. Tal como anteriormente, poderá analisar o seu computador em termos de vírus e utilizar as componentes de protecção, mas só utilizando as assinaturas de ameaças que possuía quando a licença expirou. Não podemos garantir que fique protegido dos vírus depois da licença do programa expirar.

Para evitar a infecção do seu computador com novos vírus, recomendamos o prolongamento da sua licença do Kaspersky Anti-Virus para Windows Workstations. O programa notificá-lo-á duas semanas antes da expiração da sua

licença. O programa exibirá esta mensagens durante duas semanas de cada vez que o abrir.

Para renovar a licença, precisa de comprar e instalar uma nova chave de licença para a aplicação ou introduzir um código de activação da aplicação. Para o fazer:

Contacte o distribuidor onde comprou o produto e compre uma chave de licença da aplicação ou código da aplicação.

ou:

Compre uma chave de licença ou código de activação, directamente, na Kaspersky Lab, clicando na ligação Comprar Licença na janela da chave de licença (ver Figura 96). Complete o formulário adequado no site que se abre. Depois do pagamento ser efectuado, enviaremos um link para o endereço de correio electrónico que introduziu no formulário de encomenda. Com este link, pode transferir uma chave de licença ou obter um código de activação.

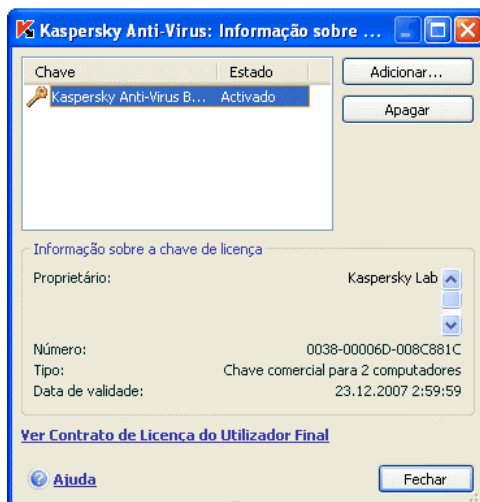



Figura 96. Informação sobre a licença

A Kaspersky Lab tem regularmente ofertas com preços especiais para os prolongamentos das licenças dos nossos produtos. Procure ofertas especiais no site da Kaspersky Lab em **Products → Sales and special offers**.

A informação acerca da chave de licença actual está disponível na caixa **Informação sobre a Licença** na secção **Serviço** da janela principal da aplicação. Para aceder à janela de gestor da licença, clique com o botão

esquerdo do rato em qualquer lugar da caixa. Na janela que se abre (ver Figura 96), pode ver informação sobre a chave actual, adicionar uma chave ou apagar uma chave.

Quando selecciona uma chave na lista da caixa **Informação sobre a Licença**, será apresentada informação sobre o número da licença, tipo de licença e data de validade da mesma. Para adicionar uma nova chave de licença, clique em **Adicionar** e active a aplicação com o assistente de activação. Para apagar uma chave da lista, clique no botão **Apagar.**

Para rever os termos do acordo de licença, clique na ligação Ver Contrato de Licença do Utilizador Final. Para obter uma licença, utilizando o formulário da Internet no site da Kaspersky Lab, clique na ligação Comprar Licença.

17.6. Suporte Técnico

O Kaspersky Anti-Virus para Windows Workstations fornece uma vasta gama de opções para as questões e problemas relacionados com o funcionamento do programa. Estão todas localizadas na secção **Suporte** (ver Figura 97) em **Serviço**.

Figura 97. Informação sobre o Suporte Técnico

Dependendo do problema, oferecemos vários serviços de Suporte Técnico:

Fórum de Utilizadores. Este recurso é uma secção dedicada do site da Kaspersky Lab com perguntas, comentários e sugestões feitas pelos utilizadores do programa. Pode explorar os tópicos básicos do fórum e deixar um comentário seu. Também poderá encontrar a resposta à sua pergunta.

Para aceder a este recurso, utilize a ligação Fórum de Utilizadores.

Base de conhecimento. Este recurso também é uma secção dedicada do site da Kaspersky Lab e contém recomendações de Suporte Técnico para a utilização do software da Kaspersky Lab e respostas às perguntas mais frequentes. Tente encontrar uma resposta à sua pergunta ou uma solução para o seu problema através deste recurso.

Para obter Suporte Técnico online, utilize a ligação Base de Conhecimento.

Comentários sobre o funcionamento do programa. Este serviço está concebido para colocar comentários sobre o funcionamento do programa ou descrever um problema que surgiu durante o funcionamento do programa. Deve preencher um formulário especial no site da empresa que descreve, detalhadamente, a situação. De forma a tratar o problema da melhor maneira, a Kaspersky Lab necessitará de informação sobre o seu computador. Poderá descrever a configuração do sistema ou utilizar o colector de informação automático no seu computador.

Para aceder ao formulário de comentários utilize a ligação Envie um relatório de erro ou uma sugestão.

Suporte Técnico. Se precisar de ajuda na utilização do Kaspersky Anti-virus, clique na ligação existente na secção **Serviço de Suporte Local**. O site da Kaspersky Lab abrir-se-á com informação sobre como contactar os nossos especialistas.

17.7. Criar uma lista de portas monitorizadas

As componente de protecção como o Anti-vírus de E-mail e o Anti-vírus de Internet, Anti-Spy e Anti-Spam são monitorizados os fluxos de dados transmitidos utilizando determinados protocolos e que passam através de determinadas portas abertas no seu computador. Assim, por exemplo, o Anti-vírus de E-mail analisa a informação transferida utilizando protocolo SMTP e o

Anti-vírus de Internet analisa a informação transferida utilizando o protocolo HTTP.

Uma lista das portas habitualmente utilizadas para transmitir e-mails e tráfego HTTP está incluída no pacote do programa. Você pode adicionar uma nova porta ou desactivar a monitorização de uma determinada porta, desactivando assim a detecção de ficheiros perigosos para o tráfego que passa através dessa porta.

Para editar a lista de portas monitorizadas, siga os seguintes passos:

1. Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations clicando na ligação Definições na janela principal.
2. Seleccione **Definições de rede** na secção **Serviço** da árvore de definições do programa.
3. Na parte direita da janela, clique em **Definições de Portas**.
4. Edite a lista das portas monitorizadas na janela que se abre (ver Figura 98).

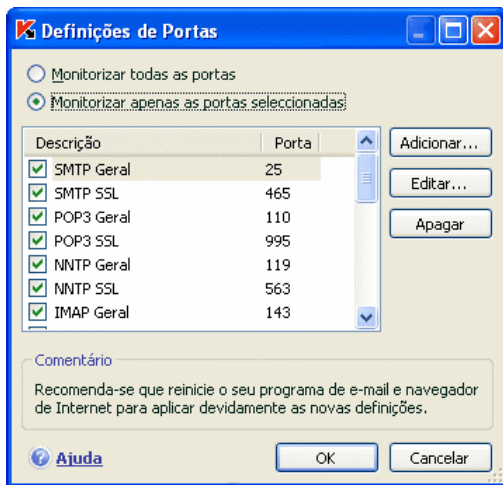



Figura 98. Lista de portas monitorizadas

Esta janela apresenta uma lista das portas monitorizadas pelo Kaspersky Anti-virus. Para analisar fluxos de dados que entrem em todas as portas de rede abertas, seleccione a opção **Monitorizar todas as portas**. Para editar manualmente a lista de portas monitorizadas, seleccione **Monitorizar apenas as portas seleccionadas**.

Não recomendamos que seleccione a opção **Monitorizar todas as portas** quando administrar o Kaspersky Anti-Virus 6.0 através do Kaspersky Administration Kit, se o mesmo estiver instalado num computador com Microsoft Windows. Caso contrário podem surgir problemas no acesso aos recursos da rede e à Internet.

Para adicionar uma nova porta à lista de portas monitorizadas:

1. Clique no botão **Adicionar** na janela **Definições de Portas**.
2. Introduza o número da porta e a descrição da mesma nos campos apropriados da janela **Nova Porta**.

Por exemplo, existe uma porta não usual no seu computador através da qual os dados são trocados com um computador remoto, utilizando o protocolo HTTP. O Anti-vírus de Internet monitoriza o tráfego HTTP. Para analisar este tráfego em relação a código malicioso, pode adicionar esta porta à lista de portas controladas.

Quando alguma destas componentes se inicia, o Kaspersky Anti-virus para Windows Workstations abre a porta 1110 como porta de audição para todas as ligações que são recebidas. Se essa porta estiver ocupada na altura, o programa selecciona a 1111, 1112, etc. como porta de audição.

Se utilizar, simultaneamente, o Kaspersky Anti-virus para Windows Workstations e uma firewall de outra empresa, deve configurar a firewall de maneira a permitir o processo *avp.exe* (processo interno do Kaspersky Anti-virus para Windows Workstations) em todas as portas acima listadas.

Por exemplo, a sua firewall contém uma regra para o *iexplorer.exe* que permite que esse processo estabeleça ligações na porta 80.

No entanto, quando o Kaspersky Anti-virus para Windows Workstations intercepta a ligação de consulta iniciada pelo *iexplorer.exe* na porta 80, ele transfere-a para o *avp.exe*, a qual por sua vez tenta estabelecer uma ligação com a página da Internet de forma independente. Se não existir uma regra de permissão para o *avp.exe*, a firewall bloqueará a consulta. Então, o utilizador não poderá aceder à página da Internet.

17.8. Verificar ligações encriptadas

A ligação por intermédio do protocolo SSL protege o intercâmbio de dados através da Internet. O protocolo SSL consegue identificar as partes que estão a trocar dados através de certificados electrónicos, codificar os dados a serem transferidos e assegurar a sua integridade durante a transferência.

Estas funcionalidades do protocolo são utilizadas por hackers para espalhar programas maliciosos, uma vez que a maior parte dos programas de anti-vírus não analisa o tráfego por SSL.

O Kaspersky Anti-virus 6.0 tem a opção de analisar o tráfego por SSL quanto à presença de vírus. Quando é feita uma tentativa para estabelecer uma ligação segura a um recurso da Internet, aparecerá uma notificação no ecrã (ver Figura 99) a perguntar ao utilizador o que fazer.

A notificação contém informação sobre o programa que está a iniciar a ligação segura, juntamente com o endereço remoto e a porta. O programa pede-lhe para decidir se aquela ligação deve ou não ser analisada em termos de vírus:

- **Processar** – analisar tráfego em termos de vírus quando estabelecer uma ligação segura com o site.

  Recomendamos que verifique sempre o tráfego por SSL se estiver a utilizar um site suspeito ou se uma transferência de dados por SSL começar quando avança para a página seguinte. É muito provável que isto seja um sinal de um programa malicioso a ser transferido através de protocolo seguro.

- **Ignorar** – continuar ligação segura com o site, sem analisar o tráfego em termos de vírus.

Para aplicar a acção seleccionada a todas as tentativas, que surjam no futuro, para estabelecer ligações por SSL, assinale a opção ☑ **Aplicar a todos**.

Figura 99. Notificação sobre a detecção de uma ligação SSL

Para analisar ligações encriptadas, o Kaspersky Anti-virus substitui o certificado de segurança solicitado por um certificado assinado pelo próprio. Nalguns casos, os programas que estão a estabelecer ligações não aceitarão este

certificado, fazendo com que não seja estabelecida nenhuma ligação. Recomendamos que desactive a verificação do tráfego de SSL nos seguintes casos:

- Ao ligar-se a um recurso de Internet confiável, como por exemplo a página de Internet do seu banco, onde gere a sua conta pessoal. Neste caso, é importante receber a confirmação da autenticidade do certificado do banco.
- Se o programa ao estabelecer a ligação verifica o certificado do site que está a aceder. Por exemplo, o MSN Messenger verifica a autenticidade da assinatura digital da Microsoft Corporation digital quando estabelece uma ligação com o servidor.

Pode configurar as definições de verificação do tráfego de SSL no separador **Definições de Rede** da janela de definições do programa:

Verificar todas as ligações encriptadas – analisa, em termos de vírus, todo o tráfego de entrada do protocolo SSL.

Perguntar ao utilizador quando for detectada uma nova ligação encriptada – apresenta uma mensagem a perguntar ao utilizador qual a acção a tomar cada vez que é estabelecida uma ligação por SSL.

Não verificar ligações encriptadas – não analisa, em termos de vírus, o tráfego de entrada do protocolo SSL.

17.9. Configurar a Interface do Kaspersky Anti-Virus para Windows Workstations

O Kaspersky Anti-virus para Windows Workstations dá-lhe a opção de alterar o aspecto do programa, criando e utilizando máscaras. Você também pode configurar a utilização de elementos de interface activos tais como o ícone de bandeja do sistema e as mensagens de popup.

Para configurar a interface do programa, siga os passos seguintes:

1. Abra a janela de definições do Kaspersky Anti-virus para Windows Workstations clicando na ligação Definições na janela principal.
2. Seleccione **Aparência** na secção **Serviço** da árvore de definições do programa (ver Figura 100).

Na parte direita da janela de definições você pode determinar:

- Se apresenta o indicador de protecção do Kaspersky Anti-virus para Windows Workstations quando o sistema operativo se inicia.

  Este indicador aparece por definição no canto superior direito do ecrã quando o programa se inicia. Ele informa-o que o seu computador está protegido contra todos os tipos de ameaças. Se não deseja utilizar o indicador de protecção, retire a selecção em ☑ **Mostrar o ícone por cima da janela de início de sessão do Windows**.

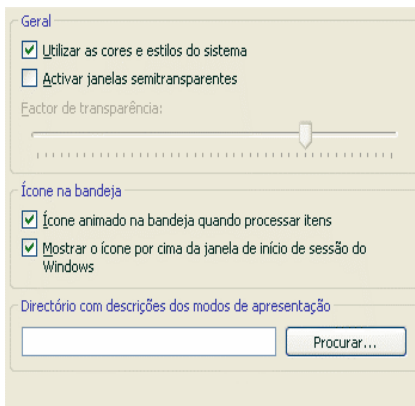



Figura 100. Configurar as definições da interface do programa

- Se utiliza animação no ícone da barra do sistema.

  Dependendo da operação do programa efectuada, o ícone da bandeja do sistema altera-se. Por exemplo, se um script estiver a ser analisado, uma pequena descrição do script aparece no fundo do ícone e se um e-mail estiver a ser analisado, surge um envelope. Por defeito, a animação do ícone é utilizada. Se deseja desactivar a animação, desmarque a opção ☑ **Ícone animado na bandeja quando processar itens**. Então o ícone só reflectirá o estado de protecção do seu computador: se a protecção estiver activada, o ícone está a cores, e se a protecção estiver suspensa ou desactivada, o ícone será cinzento.

- Grau de transparência das mensagens de popup.

  Todas as operações do Kaspersky Anti-virus para Windows Workstations que devam chegar imediatamente até si ou que necessitem da sua decisão são apresentadas como mensagens de popup sobre o ícone bandeja do sistema. As janelas da mensagem são translúcidas de forma a não interferirem com o seu trabalho. Se mover o cursor por cima da mensagem, a transparência desaparece. Você pode ajustar o grau de

transparência dessas mensagens. Para o fazer, ajuste a escala **Factor de transparência** para a posição desejada. Para remover a transparência das mensagens, desmarque a opção ☑ **Activar janelas semitransparentes**.

> Esta função não está disponível com o Windows 98/NT 4.0/ME.

- Utilize os seus próprios modos de apresentação para a interface do programa.

  Todas as cores, fontes, ícones e textos utilizados na interface do Kaspersky Anti-virus para Windows Workstations podem ser alteradas. Você pode criar os seus próprios gráficos para o programa ou pode colocá-lo numa outra linguagem. Para utilizar um modo de apresentação, especifique o directório com as suas definições no campo **Directório com descrições dos modos de apresentação**. Utilize o botão **Procurar** para seleccionar o directório.

  Por definição, as cores do sistema e os estilos são utilizados no modo de apresentação. Pode removê-los, desmarcando a opção ☑ **Utilizar as cores e estilos do sistema**. Então, serão utilizados os estilos que você especificou nas definições do tema de ecrã.

> Repare que as alterações à interface do Kaspersky Anti-virus para Windows Workstations não são guardadas se restaurar as predefinições ou desinstalar o programa.

17.10. Disco de Recuperação

O Kaspersky Anti-virus para Windows Workstations tem uma ferramenta para criar um Disco de Recuperação.

O Disco de Recuperação foi concebido para restaurar a funcionalidade do sistema depois de um ataque de vírus que danificou os ficheiros do sistema e tornou impossível o reinício do sistema operativo. Este disco inclui:

- Ficheiros do sistema Microsoft Windows XP Service Pack 2
- Um conjunto de utilidades de diagnóstico do sistema operativo
- Ficheiros do programa Kaspersky Anti-virus para Windows Workstations
- Ficheiros com assinaturas de ameaças

Para criar um Disco de Recuperação:

1. Abra a janela principal do programa e seleccione **Disco de Recuperação** na secção **Serviço**.
2. Clique no botão **Iniciar Assistente** para iniciar o processo de criação do disco.

Um Disco de Recuperação é concebido para o computador no qual foi criado. A utilização do disco de recuperação noutros computadores pode levar a consequências imprevisíveis, uma vez que contém informação acerca dos parâmetros de um computador específico (informação em sectores de arranque, por exemplo).

Apenas pode criar um disco de recuperação com o Windows XP e Microsoft Windows Vista. Não pode criar um disco de recuperação em computadores com o Microsoft Windows XP Professional Edição x64 ou Microsoft Windows Vista x64.

17.10.1. Criar um Disco de Recuperação

Aviso! Você precisa do disco de instalação do Microsoft Windows XP Service Pack 2 para criar um disco de recuperação.

Você precisa do programa **PE Builder** para criar um Disco de Recuperação.

Você precisa de instalar este PE Builder no seu computador antes de criar um disco com o mesmo.

Surgirá um Assistente especial para o guiar na criação do Disco de Recuperação. Este consiste numa série de janelas/passos e você pode navegar entre elas utilizando os botões **Anterior** e **Seguinte**. Pode finalizar o Assistente clicando em **Concluir**. O botão **Cancelar** irá parar o Assistente em qualquer ponto.

Passo 1. Preparar-se para gravar o disco

Para criar um disco de recuperação, forneça os caminhos para as seguintes pastas:

- Pasta do programa PE Builder
- Pasta onde os ficheiros do Disco de Recuperação são guardados antes de gravar o CD.

Se não estiver a criar um disco pela primeira vez, esta pasta já possuirá um conjunto de ficheiros gerados na última vez. Para utilizar os ficheiros previamente gravados, assinale a respectiva caixa.

> Repare que uma versão anterior dos ficheiros do disco de recuperação contém assinaturas de ameaça desactualizadas. Para analisar de forma correcta o computador e para restaurar o sistema, recomendamos a actualização das assinaturas de ameaça e a criação de uma nova versão do disco de recuperação.

- CD de instalação do Microsoft Windows XP Service Pack 2

Para criar um disco de recuperação com o qual possa iniciar o sistema operativo num computador remoto e verificar e processar código malicioso utilizando o Kaspersky Anti-Virus, assinale a opção ☑ **Activar administração remota para o computador recuperado**.

Note que para usar esta funcionalidade, o computador remoto tem que suportar Intel® vPRO™ ou Intel® Active Management Technology (iAMT). Estas tecnologias permitem que os administradores acedam remotamente a todos os computadores ligados à rede, incluindo aqueles que estão desligados e cujos discos rígidos falharam ou cujos sistemas operativos estão comprometidos.

Depois de introduzir os caminhos para as pastas exigidas, clique em **Seguinte**. O PE Builder arrancará e o processo de criação do Disco de Recuperação começará. Aguarde até que o processo esteja completo. Isto poderá demorar alguns minutos.

Passo 2. Criar o ficheiro .iso

Depois do PE Builder ter terminado a criação dos ficheiros do Disco de Recuperação, abrir-se-á a janela **Criar ficheiro .iso**.

O ficheiro .iso é uma imagem de CD do disco, guardado como um arquivo. A maioria dos programas de gravação de CDs reconhecem correctamente os ficheiros .iso (o Nero, por exemplo).

Se esta não for a primeira vez que cria um Disco de Recuperação, pode seleccionar o ficheiro .iso a partir do disco anterior. Para o fazer, seleccione **Utilizar um ficheiro ISO já existente**.

Passo 3. Gravar o disco

Esta janela do assistente pedir-lhe-á para escolher quando gravar os ficheiros do Disco de Recuperação para o CD: agora ou mais tarde.

Se escolher gravar o disco imediatamente, especifique se deseja formatar o CD antes de o gravar. Para o fazer, seleccione a caixa correspondente. Só terá esta opção se estiver a utilizar um CD-RW.

O CD começará a ser gravado quando clicar no botão **Seguinte**. Espere até o processo estar completo. Isto pode levar alguns minutos.

Passo 4. Concluir o Disco de Recuperação

A janela do Assistente informá-lo-á que criou com sucesso um disco de recuperação.

17.10.2. Utilizar o Disco de Recuperação

Note que o Kaspersky Anti-virus só funciona em modo de recuperação do sistema se a janela principal estiver aberta. Quando fecha a janela principal, o programa fechará.

O Bart PE, o programa predefinido, não suporta ficheiros .chm ou navegadores de Internet, por isso não poderá ver a Ajuda do Kaspersky Anti-virus ou ligações na interface do programa enquanto estiver no Modo de Recuperação.

Se surgir uma situação em que o ataque de um vírus torne impossível o carregar do sistema operativo, siga os seguintes passos:

1. Crie um disco de recuperação utilizando o Kaspersky Anti-virus para Windows Workstations num computador não infectado.
2. Introduza o disco de recuperação na unidade do disco do computador infectado e reinicie o computador. O Microsoft Windows XP SP2 iniciará a interface Bart PE. O Bart PE tem apoio de rede incorporado para utilizar a sua Rede de Área Local. Quando o programa inicia, perguntar-lhe-á se o deseja activar. Deve activar o apoio da rede se planeia actualizar as assinaturas de ameaças a partir da Rede de Área Local antes de analisar o seu computador. Se não necessita de actualizar, cancele o apoio da rede.
3. Para abrir o Kaspersky Anti-virus, clique em **Iniciar→Programas→Kaspersky Anti-Virus 6.0 para Windows Workstations →Iniciar**.

   A janela principal do Kaspersky Anti-virus para Windows Workstations abrir-se-á. No modo de recuperação do sistema, apenas poderá aceder às verificações de vírus e às actualizações das assinaturas de

ameaças a partir da Rede de Área Local (se activou o apoio da rede no Bart PE).

4. Inicie a verificação de vírus.

Note que, por defeito, são utilizadas as assinaturas de ameaças da data em que o disco de recuperação foi criado. Por essa razão, recomendamos que actualize as assinaturas antes de iniciar a verificação.

Também deve ter em conta que a aplicação apenas usará as Assinaturas de Ameaças actualizadas durante a sessão actual com o disco de recuperação, antes de reiniciar o computador.

Aviso!

Se foram detectados objectos infectados ou potencialmente infectados quando analisou o computador e se esses foram processados e depois movidos para a Quarentena ou Cópia de Segurança, recomendamos que conclua o processamento desses objectos durante a sessão actual com um disco de recuperação.

Caso contrário, perder-se-ão esses objectos quando reiniciar o seu computador.

17.11. Utilizar serviços adicionais

O Kaspersky Anti-virus para Windows Workstations fornece-lhe as seguintes funcionalidades avançadas:

- Notificações de determinados eventos que ocorrem no programa.
- A Autodefesa do Kaspersky Anti-virus para Windows Workstations no que respeita a módulos a desactivar, apagar ou editar, assim como a protecção por password para o programa.
- Resolução de conflitos com o Kaspersky Anti-virus 6.0 ao utilizar outras aplicações.

Para configurar estas funções:

1. Abra a janela de configuração do programa através da ligação Definições na janela principal.
2. Seleccione a secção **Serviço** a partir da árvore de definições.

Na parte direita do ecrã, pode definir se utilizará funcionalidades adicionais no funcionamento do programa.

17.11.1. Notificações de eventos do Kaspersky Anti-Virus para Windows Workstations

Ocorrem diferentes tipos de eventos no Kaspersky Anti-virus para Windows Workstations. Podem ser de natureza informativa ou conter informação importante. Por exemplo, um evento pode informá-lo de que o programa se actualizou com sucesso ou pode guardar um erro na componente que deve ser imediatamente eliminado.

Para receber notificações sobre o funcionamento do Kaspersky Anti-virus para Windows Workstations, pode utilizar a funcionalidade de notificação.

Os avisos podem ser entregues de diversas formas:

- Mensagens de popup por cima do ícone do programa na barra do sistema
- Mensagens sonoras
- Mensagens de e-mail
- Registo de informação no Log de eventos

Para utilizar esta funcionalidade, deve:

1. Seleccionar a opção ☑ **Activar notificações** na caixa **Interacção com o utilizador** (ver Figura 101).

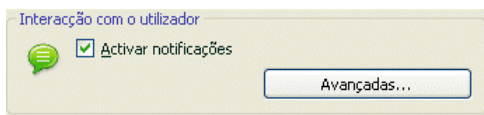



Figura 101. Activar notificações

2. Definir os tipos de eventos do Kaspersky Anti-virus para Windows Workstations, dos quais pretende notificações e o método de entrega da notificação (ver 17.11.1.1 na pág. 279).
3. Configurar as definições de entrega de notificações por e-mail, se esse for o método que está a ser utilizado (ver 17.11.1.2 na pág. 280).

17.11.1.1. Tipos de eventos e métodos de entrega das notificações

Durante o funcionamento do Kaspersky Anti-virus para Windows Workstations, surgem os seguintes tipos de eventos:

Notificações críticas são eventos de uma importância crítica. As notificações são altamente recomendadas, já que apontam problemas no funcionamento do programa ou vulnerabilidades na protecção do seu computador. Por exemplo, *assinaturas de ameaça corrompidas ou licença expirada*.

Notificações de erro – eventos que levam a que o programa não funcione. Por exemplo, *sem licença ou assinaturas de ameaças*.

Notificações importantes são eventos que devem ser investigados, já que reflectem situações importantes no funcionamento do programa. Por exemplo, *protecção desactivada ou o computador não é analisado há muito tempo.*

Notificações menores são mensagens referência - tipo que geralmente não contêm informação importante. Por exemplo, *todos os ficheiros perigosos estão desinfectados*.

Para especificar sobre que eventos o programa o deveria notificar e como:

1. Clique na ligação Definições na janela principal do programa.

2. Na janela de definições do programa, seleccione **Serviço**, assinale a opção ☑ **Activar notificações** e edite as definições detalhadas, clicando no botão **Avançadas**.

Você pode configurar os seguintes métodos de notificação para os eventos acima listados na janela **Definições de notificação** que se abre (ver Figura 102):

- *Mensagens de popup* por cima do ícone do programa na barra do sistema, que contêm uma mensagem informativa sobre o evento que aconteceu.

  Para utilizar este tipo de notificação, seleccione ☑ **Balão** à frente do evento sobre o qual deseja ser informado.

- *Notificação sonora*

  Se deseja que esta notificação seja acompanhada por um ficheiro de som, seleccione ☑ **Som** à frente do evento.

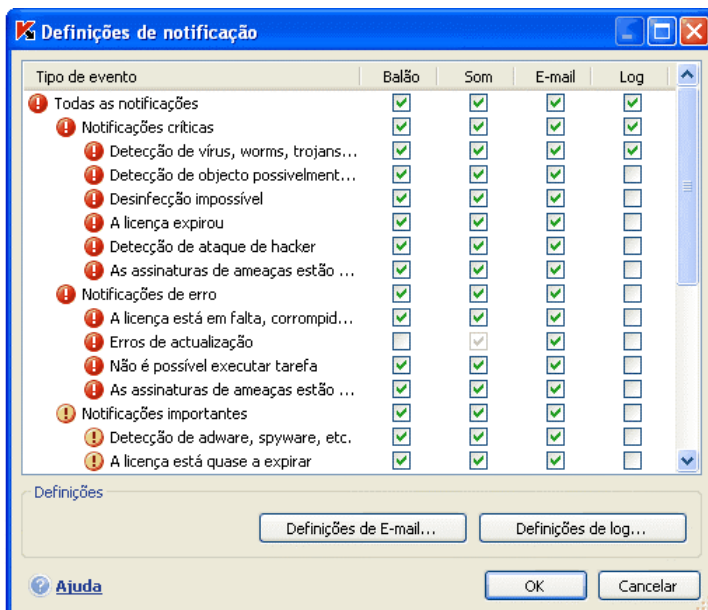
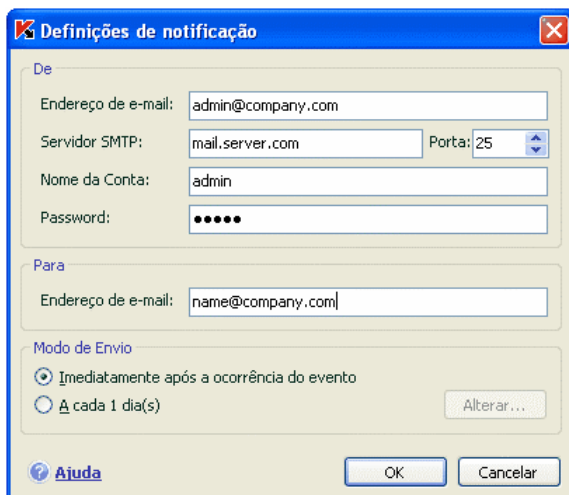



Figura 102. Eventos do programa e métodos de notificação de eventos

- *Notificação por mensagem de correio electrónico*

  Para utilizar este tipo de notificação, assinale a coluna **E-mail** à frente do evento sobre o qual deseja ser informado e configure as definições para envio de notificações (ver 17.11.1.2 na pág. 280).

- *Registo de informação no log de eventos*

  Para registar informação no registo acerca dos eventos que ocorrem, assinale a coluna **Log** e configure as definições do log de eventos (ver 17.11.1.2 na pág. 280).

17.11.1.2. Configurar notificações por e-mail

Depois de ter seleccionado os eventos (ver 17.11.1.1 na pág. 279) acerca dos quais deseja receber notificação por e-mail, deve configurar a entrega da notificação. Para o fazer:

1. Abra a janela de configuração do programa com a ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.

3. Clique em **Avançadas** na caixa **Interacção com o utilizador** na parte direita do ecrã.

4. No separador **Definições de notificação** (ver Figura 102), seleccione a caixa de selecção na coluna **E-mail** para os eventos que devem gerar uma mensagem de e-mail.

5. Na janela que se abre quando clica em **Definições de E-mail**, configure as seguintes definições para enviar notificações por e-mail:

   - Atribua a definição de envio de notificação em **De**: **Endereço de e-mail**.

   - Especifique o endereço de e-mail para o qual serão enviadas as notificações em **Para: Endereço de e-mail**.

   - Atribua um método de entrega da notificação por e-mail em **Modo de Envio**. Se deseja que o programa envie um e-mail assim que o evento ocorrer, seleccione a opção **Imediatamente após a ocorrência do evento**. Para as notificações sobre eventos com um certo período de tempo, preencha o agendamento para envio de e-mails informativos, clicando em **Alterar**. A predefinição são as notificações diárias.

Figura 103. Configurar definições de notificação por e-mail

17.11.1.3. Configurar definições de registo de eventos

Para configurar as definições do registo de eventos:

1. Abra a janela de configuração do programa com a ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.
3. Clique em **Avançadas** na secção **Interacção com o utilizador** na parte direita do ecrã.

Na janela de **Definições de notificação**, seleccione a opção para registar informação para um evento e clique no botão **Definições de log**.

O Kaspersky Anti-virus tem a opção de guardar informação acerca de eventos que ocorram enquanto o programa está a funcionar, quer no registo de eventos geral do MS Windows (**Aplicação**) ou num registo de eventos dedicado do Kaspersky Anti-virus (**Log de Eventos da Kaspersky**).

Não pode registar eventos com o Microsoft Windows 98/ME, Não pode registar no **Log de Eventos da Kaspersky** com o Microsoft Windows NT 4.0.

Estas limitações existem devido às funções destes sistemas operativos.

Os registos podem ser visualizados no **Visualizador de eventos** do MS Windows, que pode abrir acedendo a **Iniciar** → **Painel de Controlo** → **Ferramentas Administrativas** → **Visualizador de Eventos**.

17.11.2. Autodefesa e restrição de acesso

O Kaspersky Anti-virus para Windows Workstations garante a segurança do seu computador contra programas maliciosos, e por esse facto, ele pode ser o alvo de programas maliciosos que tentam bloquear o programa ou mesmo apagá-lo no computador.

Cada vez mais várias pessoas podem utilizar um PC, todas com níveis variados de conhecimento sobre computadores. Deixar aberto o acesso ao programa e às suas definições pode baixar, dramaticamente, a segurança do computador como um todo.

Para assegurar a estabilidade do sistema de segurança do seu computador, a Autodefesa, defesa de acesso remoto e os mecanismos de protecção por password foram adicionados ao programa.

A função de autodefesa da aplicação não está disponível se o Kaspersky Anti-virus estiver a funcionar com o Microsoft Windows 98/ME.

Nos computadores com sistemas operativos de 64-bit e com o Microsoft Windows Vista, a autodefesa apenas está disponível para impedir que os ficheiros do próprio programa nas unidades locais e o registo do sistema sejam alterados ou apagados.

Para activar a Autodefesa:

1. Abra a janela de definições do programa através da ligação Definições na janela principal.
2. Seleccione **Serviço** na árvore de definições.
3. Defina as seguintes configurações na caixa **Autodefesa** (ver Figura 104):

☑ **Activar Autodefesa**. Se esta caixa for seleccionada, o programa protegerá os seus próprios ficheiros, processos na memória e entradas no registo do sistema, impedindo-os de serem apagados ou modificados.

☑ **Desactivar Serviço de Controle Externo**. Se esta caixa for seleccionada, qualquer programa de administração remota que tente utilizar o programa será bloqueado.

Se alguma das acções listadas forem tentadas, aparecerá uma mensagem por cima do ícone do programa na barra do sistema (se o serviço de notificação não tiver sido desactivado pelo utilizador).

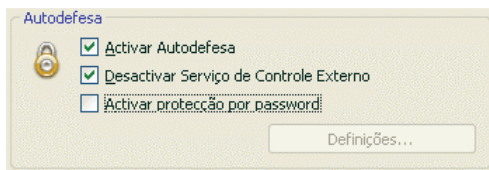



Figura 104. Configurar defesa do programa

Para proteger o programa através de uma password, seleccione **Activar protecção por password**. Clique no botão **Definições** para abrir a janela **Protecção por Password** e introduza a password e a área que a restrição de acesso abrangerá (ver Figura 105). Pode bloquear qualquer operação do programa, excepto as notificações de detecção de objectos perigosos ou evitar que alguma das seguintes acções seja efectuada:

- Alteração das definições de funcionamento do programa
- Encerramento do Kaspersky Anti-virus para Windows Workstations

- Desactivação ou pausa da protecção do seu computador

Cada uma destas acções diminui o nível de protecção do seu computador, por isso tente estabelecer em qual dos utilizadores do seu computador confia para efectuar tais acções.

Agora, sempre que um utilizador do seu computador tentar efectuar as acções que você escolheu, o programa pedirá uma password.

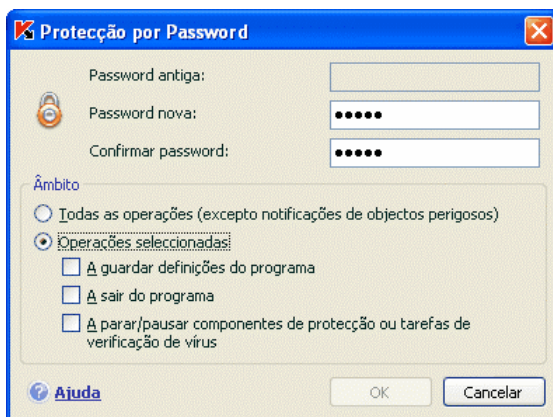



Figura 105. Definições da protecção por password do programa

17.11.3. Resolver conflitos com outras aplicações

Nalguns casos, o Kaspersky Anti-virus pode causar conflitos com outras aplicações instaladas no computador. Isso acontece porque esses programas têm mecanismos integrados de autodefesa que se activam quando o Kaspersky Anti-virus tenta inspeccioná-los. Estas aplicações incluem o plug-in Authentica para o Acrobat Reader, que verifica o acesso a ficheiros .pdf, o Oxygen Phone Manager II e alguns jogos de computador que têm ferramentas de gestão de direitos digitais.

Para corrigir este problema, assinale a opção **Modo de compatibilidade para programas através de métodos de autoprotecção** na secção **Serviço** da janela de definições da aplicação. Tem que reiniciar o seu sistema operativa para que esta alteração entre em efeito.

Se o Kaspersky Anti-Virus estiver instalado num computador com o Microsoft Windows Vista ou Microsoft Windows Vista x64, não estará disponível a resolução de problemas de compatibilidade com outras aplicações.

Contudo, note que se seleccionar essa opção, algumas funcionalidades do Kaspersky Anti-Virus, especificamente a Monitorização de Macros VBA e o Anti-Dialer, não funcionarão. Se activar alguma destas componentes, a compatibilidade com a auto-defesa da aplicação será automaticamente desactivada. Depois de activadas, estas componentes começarão a funcionar depois de reiniciar o sistema operativo.

17.12. Importar e exportar as definições do Kaspersky Anti-Virus para Windows Workstations

O Kaspersky Anti-virus para Windows Workstations permite-lhe importar e exportar definições.

Esta é uma funcionalidade útil quando, por exemplo, o programa está instalado no seu computador de casa e no seu trabalho. Você pode configurar o programa da forma que pretender em casa, guardar essas definições num disco, usar a funcionalidade de importação e carregá-las no seu computador no trabalho. As definições são guardadas num ficheiro especial de configuração.

Para exportar as actuais definições do programa:

1. Abra a janela principal do Kaspersky Anti-virus para Windows Workstations.
2. Seleccione a secção **Serviço** e clique em Definições.
3. Clique no botão **Guardar** na secção **Gestor de configuração**.
4. Insira um nome para o ficheiro de configuração e seleccione um destino para o guardar.

Para importar as definições a partir de um ficheiro de configuração:

1. Abra a janela principal do Kaspersky Anti-virus para Windows Workstations.
2. Seleccione a secção **Serviço** e clique em Definições.
3. Clique no botão **Carregar** e seleccione o ficheiro a partir do qual pretende importar as definições do Kaspersky Anti-virus para Windows Workstations.

17.13. Repor as predefinições

É sempre possível repor as predefinições do programa, que são consideradas óptimas e são recomendadas pela Kaspersky Lab. Isso pode ser feito utilizando o Assistente de Configuração.

Para repor as definições da protecção:

1. Seleccione a secção **Serviço** e clique em Definições para aceder à janela de configuração do programa.

2. Clique no botão **Restaurar** na secção **Gestor de configuração**.

A janela que se abre pede-lhe para especificar que definições devem ser restauradas para os seus valores predefinidos.

A janela lista as componentes do programa cujas definições foram alteradas pelo utilizador ou que o programa acumulou durante o treino (Anti-Hacker ou Anti-Spam). Se tiverem sido criadas definições especiais para alguma das componentes, essas também serão apresentadas na lista.

Os exemplos de definições especiais seriam as listas negras e brancas de expressões e endereços utilizadas pelo Anti-Spam, listas de endereços confiáveis e listas de números de telefone ISP confiáveis utilizadas pelo Anti-vírus de Internet e Anti-Spy, regras de exclusão criadas para as componentes do programa, filtragem de pacotes e regras de aplicações para o Anti-Hacker, e regras de aplicações para a Defesa Pró-activa.

Estas listas são normalmente alargadas de forma gradual, através da utilização alargada do programa, com base em tarefas individuais e requisitos de segurança e normalmente demoram algum tempo a criar. Por isso, recomendamos que as guarde antes de repor as definições do programa.

Por defeito, o programa guarda todas as definições personalizadas na lista (por defeito, elas estão desmarcadas). Se não precisar de guardar uma destas definições, assinale a caixa correspondente que surge antes da mesma.

Depois de terminar de configurar as definições, clique no botão **Seguinte**. O Assistente de Configuração Inicial irá abrir-se (ver 3.2 pág. 38). Siga as instruções deste assistente.

Quando você terminar o Assistente de Configuração, o nível de segurança **Recomendado** será definido para todas as componentes, excepto para as definições que você decidiu guardar quando repôs as definições. Para além disso, as definições, com as quais configurou o Assistente de Configuração, também serão aplicadas.

CAPÍTULO 18. TRABALHAR COM O PROGRAMA A PARTIR DA LINHA DE COMANDOS

Você pode utilizar o Kaspersky Anti-virus a partir de um comando de acção. Pode executar as seguintes operações:

- Iniciar, parar, pausar e retomar a actividade das componentes da aplicação
- Iniciar, parar, pausar e retomar as verificações de vírus
- Obter informação sobre o estado actual das componentes, tarefas e estatísticas sobre as mesmas
- Verificar ficheiros seleccionados
- Actualizar assinaturas de ameaças e módulos do programa
- Aceder à Ajuda para a sintaxe de acção do comando
- Aceder à Ajuda para a sintaxe do comando

A sintaxe na linha de comandos é:

```
avp.com <command> [settings]
```

Tem que aceder ao programa através do comando de acção a partir da pasta de instalação do programa ou especificando o caminho completo para avp.com.

Os seguintes elementos podem ser utilizados como **<commands>**:

ADDKEY	Activa a aplicação utilizando um ficheiro de chave (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
ACTIVATE	Activa a aplicação através da Internet, utilizando um código de activação
START	Inicia uma componente ou tarefa
PAUSE	Pausa uma componente ou tarefa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)

RESUME	Retoma uma componente ou tarefa
STOP	Pára uma componente ou tarefa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
STATUS	Mostra o estado da componente ou tarefa actualmente no ecrã
STATISTICS	Mostra as estatísticas para a componente ou tarefa no ecrã
HELP	Ajuda com a sintaxe do comando e a lista de comandos
SCAN	Analisa ficheiros em termos de vírus
UPDATE	Inicia a actualização do programa
ROLLBACK	Reverte para a última actualização do programa (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
EXIT	Fecha o programa (você só poderá executar este comando com a password atribuída na interface do programa)
IMPORT	Importa as definições de protecção do Kaspersky Anti-Virus para Windows Workstations (comando que só pode ser executado se for inserida a password atribuída através da interface do programa)
EXPORT	Exporta as definições de protecção do Kaspersky Anti-Virus para Windows Workstations

Cada comando usa as suas próprias definições específicas para aquela componente do Kaspersky Anti-virus para Windows Workstations.

18.1. Activar a aplicação

Pode activar o programa de duas formas:

- Online, utilizando um código de activação (o comando ACTIVATE).
- Utilizando um ficheiro de chave de licença (o comando ADDKEY).

Sintaxe do comando:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Descrição de parâmetro:

<file_name>	Nome do ficheiro de chave de licença com a extensão *.key.
<activation_code>	Código de activação do programa fornecido quando o adquiriu.
<password>	Password para aceder ao Kaspersky Anti-Virus, atribuída na interface da aplicação.
Note que este comando não será aceite sem uma password.	

Exemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

18.2. Gerir componentes e tarefas do programa

Sintaxe do comando:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parâmetros:

<command>	Você pode gerir as componentes e tarefas do Kaspersky Anti-virus a partir do comando de acção com estes comandos: **START** – iniciar uma componente de protecção em tempo real ou tarefa. **STOP** – parar uma componente de protecção em tempo real ou tarefa. **PAUSE** – pausar uma componente de protecção em tempo real ou tarefa. **RESUME** – retomar uma componente de protecção em tempo real ou tarefa. **STATUS** – apresentar o actual estado da componente de protecção em tempo real ou tarefa. **STATISTICS** – apresenta estatísticas no ecrã sobre o funcionamento da componente de protecção em tempo real ou tarefa. Note que os comandos PAUSE e STOP estão protegidos por password.
<profile|task_name>	O parâmetro **<profile>** pode ser atribuído a qualquer componente de protecção em tempo real, módulos das componentes, tarefas de verificação a pedido ou actualizações como valor (os valores padrão utilizados no programa são apresentados na tabela abaixo apresentada). Os valores válidos para o parâmetro **<task_name>** podem incluir o nome de qualquer tarefa de verificação ou actualização a pedido definida pelo utilizador.
<your_password>	A password do Kaspersky Anti-Virus atribuída na interface do programa.

/R[A]:<report_file>	**R:<report_file>**: apenas regista eventos importantes no relatório. **/RA:<report_file>**: regista todos os eventos no relatório. Pode utilizar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.

Um dos seguintes valores é atribuído a **`<profile>`**:

`RTP`	Todas as componentes de protecção O comando avp.com START RTP inicia todas as todas as componentes de protecção em tempo real, se a protecção estiver desactivada por completo (ver 6.1.2 na pág. 73) ou pausada (ver 6.1.1 na pág. 72). Este comando também iniciará qualquer componente de protecção em tempo real que foi pausada utilizando o botão ▮▮ a partir da interface gráfica do utilizador ou com o comando PAUSE a partir da linha de comandos. Se a componente foi desactivada utilizando o botão ■ a partir da interface gráfica do utilizador ou com o comando STOP a partir da linha de comandos, o comando avp.com START RTP não irá iniciá-la. Para a iniciar, tem que executar o comando avp.com START <profile>, com o valor para a componente de protecção específica inserido para <profile>. Por exemplo, avp.com START FM.
`FM`	Anti-vírus de Ficheiros
`EM`	Anti-vírus de E-mail

WM	Anti-vírus de Internet Valores para as subcomponentes do Anti-vírus de Internet: **httpscan** – verifica tráfego de http **sc** – verifica scripts
BM	Defesa Pró-activa Valores para as subcomponentes da Defesa Pró-activa: **og** – análise de macros do Microsoft Office **pdm** – análise da actividade das aplicações
ASPY	Anti-Spy Valores para as subcomponentes do Anti-Spy: **AdBlocker** – AdBlocker **antidial** – Anti-Dialer **antiphishing** – Anti-Phishing **popupchk** – Bloqueador de popups
AH	Anti-Hacker Valores para as subcomponentes do Anti-Hacker: **fw** – Firewall **ids** – Sistema de Detecção de Intrusões
AS	Anti-Spam
UPDATER	Actualizador
RetranslationCfg	Distribuição de actualizações numa origem local
Rollback	Reverte para a actualização anterior
SCAN_OBJECTS	Tarefa de verificação de vírus

SCAN_MY_COMPUTER	Tarefa O Meu Computador
SCAN_CRITICAL_AREAS	Tarefa Áreas Críticas
SCAN_STARTUP	Tarefa Objectos de Inicialização
SCAN_QUARANTINE	Tarefa para verificação de objectos da quarentena
As componentes e tarefas iniciadas a partir do comando de acção trabalham com as definições configuradas na interface do programa.	

Exemplos:

Para activar o Anti-vírus de Ficheiros, digite isto na linha de comandos:

```
avp.com START FM
```

Para visualizar o estado actual da Defesa Pró-activa no seu computador, digite o seguinte texto na linha de comandos:

```
avp.com STATUS BM
```

Para parar uma tarefa de verificação "O Meu Computador" a partir da linha de comandos, introduza:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

18.3. Verificação Anti-vírus

A sintaxe para iniciar uma verificação de vírus de determinada área e processar ficheiros maliciosos a partir de um comando de acção tem, geralmente, o seguinte aspecto:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>] [<re-
port settings>] [<advanced settings>]
```

Para analisar ficheiros, você também pode utilizar as tarefas criadas no Kaspersky Anti-virus para Windows Workstations, iniciando a tarefa que necessita a partir da linha de comandos (ver 18.1 na pág. 289). A tarefa será executada com as definições especificadas na interface do programa.

Descrição de parâmetro.

<table>
<tr><td colspan="2"><object scanned> - este parâmetro dá-lhe a lista de ficheiros que serão analisados em termos de código malicioso.
Pode incluir vários valores da lista fornecida, separados por espaços.</td></tr>
<tr><td><files></td><td>Lista de caminhos para os ficheiros e/ou pastas a serem analisados. Pode introduzir caminhos absolutos ou relativos. Os itens da lista estão separados por um espaço.
Notas:
• Se o nome do ficheiro tiver um espaço, deve ser colocado entre aspas
• Se seleccionar uma pasta específica, todos os ficheiros existentes na mesma serão analisados.</td></tr>
<tr><td>/MEMORY</td><td>Objectos da memória do sistema</td></tr>
<tr><td>/STARTUP</td><td>Objectos de inicialização</td></tr>
<tr><td>/MAIL</td><td>Bases de dados de e-mails</td></tr>
<tr><td>/REMDRIVES</td><td>Todos os discos removíveis</td></tr>
<tr><td>/FIXDRIVES</td><td>Todos os discos rígidos</td></tr>
<tr><td>/NETDRIVES</td><td>Todos os discos de rede</td></tr>
<tr><td>/QUARANTINE</td><td>Objectos em quarentena</td></tr>
<tr><td>/ALL</td><td>Verificação completa</td></tr>
<tr><td>/@:<filelist.lst></td><td>Caminho para um ficheiro com uma lista de objectos e pastas a serem incluídos na verificação. O ficheiro deve estar em formato texto e cada objecto de verificação deve iniciar uma linha nova.
Pode introduzir um caminho absoluto ou relativo para o objecto. O caminho deve ser colocado entre aspas se tiver um espaço.</td></tr>
</table>

<action> - este parâmetro define respostas aos objectos maliciosos detectados durante a verificação. Se este parâmetro não for definido, o valor predefinido é **/i8**.	
/i0	Não actua sobre o objecto; simplesmente guarda informação sobre o mesmo no relatório.
/i1	Trata objectos infectados e, se a desinfecção falhar, ignora-os.
/i2	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Excepções: não apaga objectos infectados de objectos compostos e apaga objectos compostos com cabeçalhos executáveis (arquivos sfx) (esta é a predefinição).
/i3	Trata objectos infectados e, se a desinfecção falhar, apaga-os. Para além disso, apaga completamente todos os objectos compostos se os conteúdos infectados não puderem ser apagados.
/i4	Apaga objectos infectados e, se a desinfecção falhar, apaga-os. Para além disso, apaga completamente todos os objectos compostos se os conteúdos infectados não puderem ser apagados.
/i8	Solicitar a acção a efectuar se for detectado um objecto infectado.
/i9	Solicitar a acção a efectuar no final da verificação.
<file types> - este parâmetro define os tipos de ficheiros que serão sujeitos à verificação do anti-vírus. Se este parâmetro não estiver definido, o valor por defeito é /fi.	
/fe	Verifica por extensão só os ficheiros potencialmente infectados
/fi	Verifica por conteúdo só os ficheiros potencialmente infectados (opção predefinida)
/fa	Verifica todos os ficheiros

<table>
<tr><td colspan="2"><exclusions> - este parâmetro define os objectos excluídos da verificação.

Pode incluir vários valores a partir da lista fornecida, separados por espaços.</td></tr>
<tr><td>-e:a</td><td>Não verifica arquivos</td></tr>
<tr><td>-e:b</td><td>Não verifica bases de dados de e-mails</td></tr>
<tr><td>-e:m</td><td>Não verifica e-mail com texto simples</td></tr>
<tr><td>-e:<filemask></td><td>Não verifica ficheiros por máscara</td></tr>
<tr><td>-e:<seconds></td><td>Ignora os ficheiros que são verificados durante um tempo superior àquele especificado no parâmetro <seconds> (segundos).</td></tr>
<tr><td>-es:<size></td><td>Ignora ficheiros com tamanho superior (em MB) ao valor atribuído por <tamanho>.</td></tr>
<tr><td colspan="2"><configuration file> - define o caminho para o ficheiro de configuração que contém as definições do programa para a verificação.

O ficheiro de configuração é guardado em formato binário (.dat), a não ser que tenha sido especificado outro formato ou se o formato não estiver atribuído e pode ser usado mais tarde para importar definições da aplicação para outros computadores.

Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores definidos na interface do Kaspersky Anti-virus para Windows Workstations.</td></tr>
<tr><td>/C:<file_name></td><td>Utiliza os valores das definições atribuídas no ficheiro de configuração <file_name></td></tr>
<tr><td colspan="2"><report settings> - este parâmetro determina o formato do relatório sobre os resultados da verificação.

Pode usar um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.</td></tr>
<tr><td>/R:<report_file></td><td>Só regista eventos importantes neste ficheiro</td></tr>
<tr><td>/RA:<report_file></td><td>Regista todos os eventos neste ficheiro</td></tr>
</table>

<table>
<tr><td colspan="2"><Advanced settings> – definições que determinam a utilização das tecnologias de verificação anti-vírus.</td></tr>
<tr><td>/iChecker=<on|off></td><td>Activar/ desactivar iChecker.</td></tr>
<tr><td>/iSwift=<on|off></td><td>Activar/ desactivar iSwift.</td></tr>
</table>

Exemplos:

*Iniciar uma verificação da RAM, Programas de Inicialização, bases de dados do e-mails, os directórios **Os Meus Documentos** e **Ficheiros de Programa** e o ficheiro **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Pausar a verificação dos objectos seleccionados e iniciar a verificação completa do computador e depois continuar a verificação de vírus dentro dos ficheiros seleccionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Analisar a RAM e os objectos listados no ficheiro **object2scan.txt**. Utilizar o ficheiro de configuração **scan_setting.txt**. Depois da verificação, gerar um relatório em que são guardados todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Uma amostra de um ficheiro de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

18.4. Actualizações do programa

A sintaxe para actualizar os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-virus para Windows Workstations a partir do comando de acção é a seguinte:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP=<on|off>]
```

Descrição do parâmetro:

<update_source>	Servidor HTTT ou FTP ou directório de rede para transferir actualizações. Pode especificar o caminho absoluto para a origem de actualização ou um URL como o valor deste parâmetro. Se não for especificado nenhum caminho, a origem de actualização será copiada das definições de actualização.
/R[A]:<report_file>	**/R:<report_file>** – só regista eventos importantes no relatório. **/R[A]:<report_file>** – regista todos os eventos no relatório. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
/C:<file_name>	Caminho para o ficheiro de configuração com as definições das actualizações do programa. O ficheiro de configuração é um ficheiro de texto que contém um conjunto de definições da linha de comandos para a actualização do programa. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, são utilizados os valores das definições configuradas na interface do Kaspersky Anti-virus para Windows Workstations.
/APP=<on|off>	Activar / Desactivar actualizações dos módulos da aplicação

Exemplos:

Actualizar assinaturas de ameaças e gravar todos os eventos no relatório:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Actualizar os módulos do programa Kaspersky Anti-virus para Windows Workstations utilizando as definições no ficheiro de configuração **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Uma amostra de um ficheiro de configuração:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

18.5. Definições de reversão

Sintaxe do comando:

```
ROLLBACK
[/R[A]:<report_file>][/password=<your_password>]
```

/R[A]:<report_file>	**/R:<report_file>** – só regista eventos importantes no relatório. **/R[A]:<report_file>** – regista todos os eventos no relatório. Pode introduzir um caminho absoluto ou relativo para o ficheiro. Se o parâmetro não estiver definido, os resultados da verificação são exibidos no ecrã e todos os eventos são apresentados.
<your_password>	Password para aceder ao Kaspersky Anti-Virus, atribuída na interface da aplicação.
Note que não pode executar este comando sem inserir a password.	

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<your_password>
```

18.6. Exportar definições

Sintaxe do comando:

```
avp.com EXPORT <profile> <file_name>
```

Descrição do parâmetro:

<profile>	Componente ou tarefa com as definições a ser exportadas. Pode utilizar qualquer valor para **<profile>** que está listado na secção 18.2 na pág. 289.
<filename>	O ficheiro de configuração pode ser guardado como um ficheiro de texto. Para o fazer, especifique a extensão *.txt* no nome do ficheiro. Também pode guardar o ficheiro em qualquer formato binário. O ficheiro de configuração é guardado em formato binário (*.dat*), a não ser que tenha sido especificado outro formato ou se o formato não estiver atribuído e pode ser usado mais tarde para importar definições da aplicação para outros computadores. O ficheiro de configuração pode ser guardado como um ficheiro de texto. Para o fazer, especifique a extensão *.txt* no nome do ficheiro. Note que não pode importar as definições de protecção a partir de um ficheiro de texto. Este ficheiro apenas pode ser usado para especificar as principais definições do funcionamento do programa.

Exemplo:

```
avp.com EXPORT c:\settings.dat
```

18.7. Importar definições

Sintaxe do comando:

```
avp.com IMPORT <filename> [/password=<your_password>]
```

<filename>	O ficheiro de configuração pode ser guardado como um ficheiro de texto. Para o fazer, especifique a extensão *.dat* no nome do ficheiro. As definições só podem ser importadas a partir de ficheiros binários. Se instalar o programa em modo oculto a partir da linha de comandos ou com o Editor de Objectos de Política de Grupo, então o nome do ficheiro de configuração deve ser *install.cfg*. Caso contrário, o programa não irá reconhecê-lo.
<your_password>	Password para o Kaspersky Anti-virus atribuída na interface da aplicação.
Note que este comando não será aceite sem uma password.	

Exemplo:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

18.8. Iniciar o programa

Sintaxe do comando:

```
avp.com
```

18.9. Parar o programa

Sintaxe do comando:

```
avp.com EXIT /password=<your_password>
```

<your_password>	A password do Kaspersky Anti-virus para Windows Workstations atribuída na interface do programa.
Note que este comando não será aceite sem uma password.	

Note que não pode executar este comando sem introduzir uma password.

18.10. Obter um Ficheiro de Rastreio

Você pode precisar de criar um ficheiro de rastreio se tiver problemas com a execução da aplicação para resolvê-los com maior exactidão com os especialistas do Suporte Técnico.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

[on|off]	Activar/desactivar criação de ficheiro de rastreio.
[file]	Obter um rastreio e guardar num ficheiro.
<trace_level>	Este parâmetro pode ter atribuídos valores numéricos de 0 (nível mínimo, apenas eventos críticos) a 700 (nível máximo, todos os eventos). Um especialista dir-lhe-á que nível de rastreio necessita quando contactar o Suporte. Se isso não for especificado, recomendamos que configure o nível para 500.

Aviso: Apenas recomendamos a criação de ficheiros de rastreio para a resolução de um problema específico. A activação regular dos ficheiros de rastreio pode tornar o seu computador mais lento e encher o seu disco rígido.

Exemplos:

Para desactivar rastreio:

```
avp.com TRACE file off
```

Para criar um ficheiro de rastreio para enviar ao Suporte Técnico com um nível de rastreio máximo de 500:

```
avp.com TRACE file on 500
```

18.11. Visualizar o Menu Ajuda

Este comando está disponível para visualizar o Menu Ajuda sobre a sintaxe do comando de acção:

```
avp.com [ /? | HELP ]
```

Para pedir ajuda sobre a sintaxe de um comando específico, pode utilizar um dos seguintes comandos:

```
avp.com <command> /?
avp.com HELP <command>
```

18.12. Códigos de retorno da interface da linha de comandos

Esta secção contém uma lista dos códigos de retorno da linha de comandos. Os códigos gerais podem ser devolvidos por qualquer comando da linha de comandos. Os códigos de retorno incluem códigos gerais, assim como códigos específicos de um tipo de tarefa específico.

Códigos de retorno gerais	
0	Operação concluída com sucesso
1	Valor de definição inválido
2	Erro desconhecido
3	Erro de conclusão da tarefa
4	Tarefa cancelada
Códigos de retorno das tarefas de verificação do Anti-virus	
101	Todos os objectos perigosos foram processados
102	Objectos perigosos detectados

CAPÍTULO 19. MODIFICAR, REPARAR E REMOVER O PROGRAMA

Pode desinstalar a aplicação das seguintes formas:

- Usando o Assistente de Instalação (ver 19.2 na pág. 307)
- A partir da linha de comandos (ver 19.2 na pág. 307)
- Usando o Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration Kit)
- Usando as políticas de domínios de grupos do Microsoft Windows Server 2000/2003 (ver 3.4.3 na pág. 50).

19.1. Modificar, reparar e remover o programa com o Assistente de Instalação

Você poderá precisar de reparar o programa se detectar erros no seu funcionamento depois de uma configuração incorrecta ou corrupção de um ficheiro.

A modificação do programa pode instalar as componentes em falta do Kaspersky Anti-virus para Windows Workstations ou apagar aquelas que você não quer.

Para reparar ou modificar as componentes em falta do Kaspersky Anti-virus para Windows Workstations ou apagar o programa:

1. Saia do programa. Para o fazer, clique com o botão esquerdo do rato no ícone do programa na bandeja do sistema e seleccione **Sair** no menu de contexto.
2. Introduza o CD de instalação na unidade de CD-ROM, se utilizou um CD para instalar o programa. Se instalou o Kaspersky Anti-virus para Windows Workstations a partir de uma origem diferente (pasta de acesso público, pasta no disco rígido, etc.), certifique-se de que o pacote de instalação está na pasta e que você pode aceder ao mesmo.

3. Seleccione **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0 para Windows Workstations** → **Modificar, Reparar** ou **Remover**.

Um assistente de instalação abrir-se-á. Vejamos, mais detalhadamente, os passos para reparar, modificar ou apagar o programa.

Passo 1. Janela de Boas-vindas da instalação

Se seguir todos os passos acima mencionados, necessários para reparar ou modificar o programa, aparecerá a janela de boas-vindas da instalação do Kaspersky Anti-virus para Windows Workstations. Para continuar, clique no botão **Seguinte**.

Passo 2. Seleccionar uma operação

Neste passo, selecciona a operação que deseja executar. Pode modificar as componentes do programa, reparar as componentes existentes ou remover componentes ou o programa todo. Para efectuar a operação de que necessita, clique no botão apropriado. A resposta do programa depende da operação que seleccionar.

Modificar o programa é semelhante a personalizar a instalação do programa, onde pode especificar que componentes deseja instalar (ver Passo 7. na pág. 36) e quais deseja apagar.

A reparação do programa depende das componentes do programa instaladas. Os ficheiros serão reparados para todas as componentes instaladas e o nível de segurança Recomendado será configurado para cada uma delas.

Se remover o programa, pode seleccionar que dados criados e utilizados pelo programa deseja guardar no seu computador. Para apagar todos os dados do Kaspersky Anti-virus para Windows Workstations, seleccione **Concluir desinstalação**. Para guardar dados, seleccionar **Guardar os objectos da aplicação** e especifique que objectos não deseja apagar:

- *Dados de activação* – chave de licença necessária para a aplicação funcionar.
- *Assinaturas de ameaças* – conjunto completo das assinaturas de programas perigosos, vírus e outras ameaças actuais desde a última actualização.
- *Base de dados de Anti-Spam* – base de dados utilizada para detectar e-mails considerados como lixo electrónico. Esta base de dados contém informação detalhada sobre que e-mails são spam e não-spam.

- *Ficheiros de Cópia de Segurança* – cópias de segurança de ficheiros apagados ou desinfectados. Recomenda-se que sejam guardados, caso possam ser restaurados mais tarde.
- *Ficheiros de Quarentena* – ficheiros que estão potencialmente infectados por vírus ou modificações de vírus. Estes ficheiros contêm código similar ao código de um vírus conhecido, mas é difícil determinar se são maliciosos. Recomenda-se que sejam guardados, uma vez que, na verdade, podem não estar infectados ou podem ser desinfectados depois da actualização das assinaturas de ameaças.
- *Definições da aplicação* – configurações para todas as componentes do programa.
- *Dados do iSwift* – base de dados com informação sobre ficheiros verificados em sistemas de ficheiros NTFS. Isto pode aumentar a velocidade de verificação. Quando utiliza esta base de dados, o Kaspersky Anti-Virus para Windows Workstations só analisa os ficheiros que foram modificados desde a ultima verificação.

> Aviso!
>
> Se passar um longo período de tempo entre a desinstalação de uma versão do Kaspersky Anti-virus para Windows Workstations e a instalação de uma outra versão, não recomendamos a utilização da base de dados do *iSwift* de uma instalação anterior. Um programa perigoso poderá penetrar no computador durante este período e os seus efeitos não seriam detectados pela base de dados, o que poderia levar a uma infecção.

Para iniciar a operação seleccionada, clique no botão **Seguinte**. O programa começará a copiar os ficheiros necessários para o seu computador ou a apagar as componentes e dados seleccionados.

Passo 3. Concluir a modificação, reparação ou remoção do programa

O processo de modificação, reparação ou remoção será mostrado no ecrã, após o qual você será informado da sua conclusão.

Normalmente, a remoção do programa implica que reinicie o seu computador, já que isso é necessário para assumir as modificações ao seu sistema. O programa pedir-lhe-á para reiniciar o seu computador. Clique em **Sim** para reiniciar imediatamente. Para reiniciar o seu computador mais tarde, clique em **Não**.

19.2. Desinstalar o programa a partir da linha de comandos

Para desinstalar o Kaspersky Anti-Virus 6.0 para Windows Workstations a partir da linha de comandos, introduza:

```
msiexec /x <package_name>
```

O assistente de instalação abrir-se-á. Pode usá-lo para desinstalar a aplicação (ver Capítulo 19 na pág. 304).

Para desinstalar a aplicação no modo não interactivo sem reiniciar o computador (o computador deverá ser manualmente reiniciado depois da instalação), digite:

```
msiexec /x <package_name> /qn
```

Para desinstalar a aplicação no modo não interactivo e depois reiniciar o computador, digite:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

Se, ao instalar o programa, optou por proteger com password a desinstalação do programa, é necessário introduzir esta password. Caso contrário, o programa não poderá ser desinstalado.

Para remover a aplicação, introduzindo uma password como prova do privilégio de remoção, digite:

`msiexec /x <package_name> KLUNINSTPASSWD=******` – para remover a aplicação no modo interactivo;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – para remover a aplicação no modo não interactivo;

CAPÍTULO 20. ADMINISTRAR O PROGRAMA COM O KASPERSKY ADMINISTRATION KIT

O **Kaspersky Administration Kit** é um sistema para gerir, de forma centralizada, as tarefas administrativas com chaves na operação de um sistema de segurança para uma rede empresarial, com base nas aplicações incluídas nas soluções Kaspersky Anti-Virus Business Optimal e Kaspersky Corporate Suite.

O Kaspersky Anti-Virus 6.0 para Windows Workstations é um dos produtos da Kaspersky Lab que pode ser administrado através da sua própria interface, a linha de comandos (estes métodos são descritos acima neste Manual do Utilizador) ou através do Kaspersky Administration Kit (se o computador fizer parte do sistema centralizado de administração remota).

Execute os seguintes passos para gerir o Kaspersky Anti-Virus 6.0 para Windows Workstations através do Kaspersky Administration Kit:

- Instale o *Servidor de Administração* na rede; instale a *Consola de Administração* no local de trabalho do administrador (para mais detalhes, veja o Manual do Administrador para a instalação do Kaspersky Administration Kit 6.0);
- Instale o Kaspersky Anti-Virus 6.0 para Windows Workstations e *Administration Agent* (incluído com o Kaspersky Administration Kit) em computadores da rede. Para mais detalhes sobre a instalação remota do Kaspersky Anti-Virus em computadores da rede, veja o Guia do Administrador para a instalação do Kaspersky Administration Kit 6.0.

Tenha em atenção as seguintes especificidades na utilização do Kaspersky Anti-Virus através do Kaspersky Administration Kit:

Se os computadores na rede têm instalado o Kaspersky Anti-Virus 5.0, você deve seguir os seguintes passos antes de actualizar para a versão 6.0 através do Kaspersky Administration Kit:

- Primeiro, pare a versão anterior da aplicação (você pode fazê-lo de forma remota através do Kaspersky Administration Kit);
- Feche todas as outras aplicações antes de começar a instalação;
- Reinicie o sistema operativo no computador remoto depois da instalação estar concluída.

Depois de actualizar a extensão de administração da Kaspersky Lab através do Kaspersky Administration Kit, encerre a Consola de Administração.

A *Consola de Administração* (ver Figura 106) permite-lhe administrar a aplicação através do Kaspersky Administration Kit. Fornece uma **Interface Integrada MMC** padrão e permite ao administrador executar as seguintes funções:

- Instalar de forma remota o Kaspersky Anti-Virus 6.0 para Windows Workstations e *Administration Agent* em computadores da rede
- Configurar de forma remota o Kaspersky Anti-Virus em computadores da rede
- Actualizar as assinaturas de ameaças e módulos do Kaspersky Anti-Virus
- Gerir licenças para a aplicação em computadores da rede
- Ver informação acerca do funcionamento do programa em computadores cliente

Quando administrar o programa de forma centralizada através do Kaspersky Administration Kit, o administrador determina as definições para políticas, tarefas e aplicações. A protecção é concebida em torno destas definições.

As **Definições da Aplicação** são um conjunto de definições gerais para o funcionamento do programa, incluindo definições de protecção geral, definições da Cópia de Segurança, etc.

A **Tarefa** é uma acção específica executada pela aplicação. As tarefas do Kaspersky Anti-Virus para Windows Workstations são divididas por tipo (tarefas de instalação de chaves de licença, tarefas de verificação por pedido, tarefas de reversão de actualização das bases de dados anti-vírus, tarefas de actualização dos módulos da aplicação e das bases de dados anti-vírus). Cada tarefa específica tem um conjunto de definições do Kaspersky Anti-Virus que são usadas quando a tarefa é executada *(definições da tarefa)*.

Figura 106. Consola de Administração do Kaspersky Administration Kit

A função-chave da administração centralizada é o agrupamento de computadores remotos e a gestão das suas definições através da criação e configuração de políticas de grupo.

Uma **Política** refere-se a um conjunto de definições para o funcionamento do Kaspersky Anti-Virus no âmbito de um grupo de rede. A política também pode incluir restrições sobre a alteração das configurações atribuídas ao configurar a aplicação ou tarefa.

Uma política permite-lhe gerir a funcionalidade completa da aplicação, uma vez que contêm definições para a aplicação e para todos os tipos de tarefas, com excepção das definições que têm que ser configuradas directamente quando se inicia uma tarefa (por exemplo, agendamentos de tarefa).

20.1. Administrar a aplicação

O Kaspersky Administration Kit dá-lhe a oportunidade de parar e pausar, de forma remota, o Kaspersky Anti-Virus em computadores clientes individuais, assim como configurar definições gerais para a aplicação, tais como a activação/desactivação da protecção do computador, a configuração de

definições da Cópia de Segurança e Quarentena e a configuração de definições para a produção de relatórios.

Para gerir as definições da aplicação:

1. Seleccione a pasta do grupo que contém o computador cliente na pasta **Grupos** (ver Figura 106).
2. Na janela que se abre, seleccione o computador para o qual você precisa de modificar as definições da aplicação. No menu de contexto ou no menu **Acções**, seleccione o comando **Aplicações**.
3. O separador **Aplicações** na janela de propriedades do computador cliente (ver Figura 107) apresenta uma lista completa das aplicações da Kaspersky Lab instaladas no computador cliente. Seleccione o **Kaspersky Anti-Virus 6.0 para Windows Workstations**.

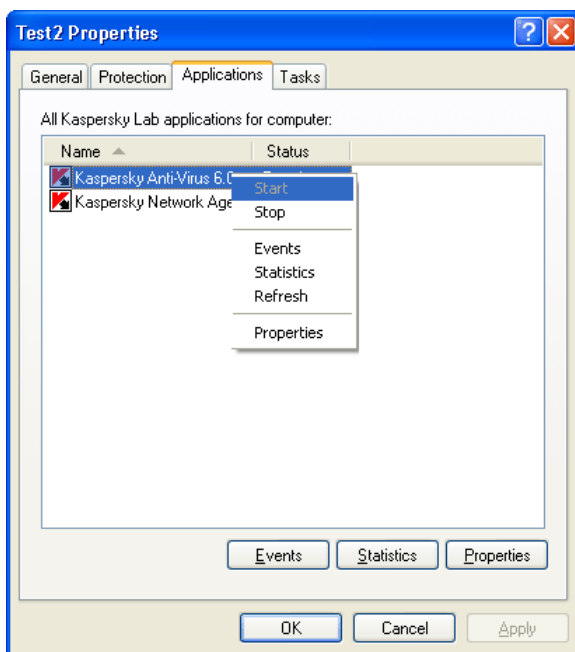



Figura 107. Lista de aplicações da Kaspersky Lab

Existem botões por baixo da lista, os quais pode utilizar para:

- Ver uma lista de eventos no funcionamento da aplicação que ocorreram no servidor e que foram guardadas no Servidor de Administração
- Ver informação estatística sobre o funcionamento da aplicação

- Configurar as definições da aplicação (ver 20.1.2 na pág. 313)

20.1.1. Iniciar/parar a aplicação

Pode iniciar ou pausar o Kaspersky Anti-Virus num computador remoto, utilizando os comandos do menu de contexto na janela **Propriedades do Nome do Computador** (ver Figura 107).

Também pode fazer isto, utilizando os botões **Iniciar/Parar** na janela de definições no separador **Geral** (ver Figura 109).

Na parte superior da janela, vai encontrar o nome da aplicação instalada, informação sobre a versão, a data de instalação, o seu estado (se a aplicação está em execução ou pausada no computador local) e informação acerca do estado da base de dados de assinaturas de ameaças.

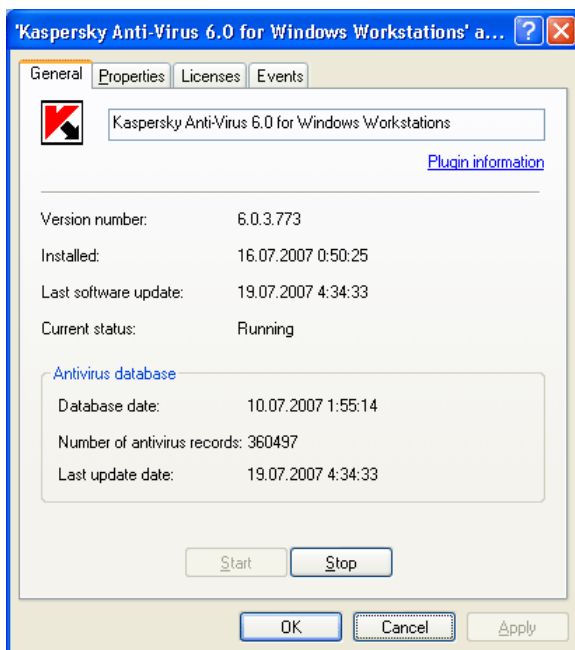



Figura 108. Configurar as definições do Kaspersky Anti-Virus. Separador **Geral**

20.1.2. Configurar as definições da aplicação

Para ver ou alterar as definições da aplicação:

1. Abra a janela de propriedades para o computador cliente no separador **Aplicações** (ver Figura 107).
2. Seleccione o **Kaspersky Anti-Virus 6.0 para Windows Workstations**. Clique no botão **Propriedades** para abrir a janela de definições da aplicação (ver Figura 109).

Todos os separadores, com excepção do separador **Propriedades,** são separadores padrão para o Kaspersky Administration Kit. Para mais informação sobre os separadores padrão, veja o Guia do Administrador.

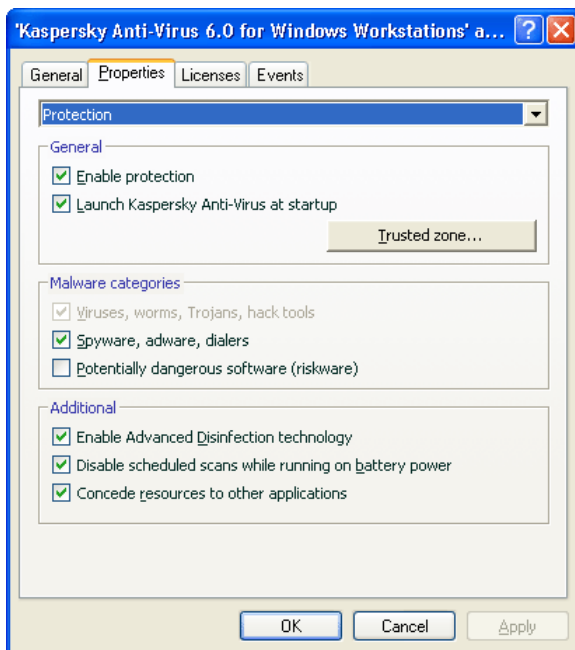



Figura 109. Configurar as definições do Kaspersky Anti-Virus. Separador **Propriedades**

Se tiver sido criada uma política para a aplicação (ver 20.3.1 na pág. 323) que impede que algumas definições sejam reconfiguradas, estas não serão editáveis ao configurar a aplicação.

No separador **Propriedades**, pode configurar as definições gerais de protecção, as definições das ferramentas de protecção da aplicação e as definições para a criar e guardar estatísticas de relatório para a aplicação. Para o fazer, seleccione o valor necessário do menu suspenso na parte superior da janela e configure as definições.

Protecção
No separador **Propriedades** na secção **Protecção**, você pode: • Activar/desactivar a protecção para um computador (ver 6.1 na pág. 71); • Configurar a inicialização automática para a aplicação quando o computador for ligado (ver 6.1.5 na pág. 75); • Criar uma zona confiável ou uma lista de exclusões (ver 6.3 na pág. 77); • Seleccionar os tipos de programas maliciosos que a aplicação irá monitorizar (ver 6.2 na pág. 76); • Configurar definições de produtividade para a aplicação e definições de configuração multi-processador (ver 6.6 na pág. 90).
Serviço
No separador **Propriedades** na secção **Serviço**, você pode: • Configurar notificações para eventos que ocorram (ver 17.11.1.2 na pág. 280) • Gerir a função de auto-defesa da aplicação e a protecção das definições da aplicação através de password (ver 17.11.1.3 na pág. 282) • Configurar a aparência da aplicação (ver 20.3.1 na pág. 323) • Configurar definições de compatibilidade entre o Kaspersky Anti-Virus e outros programa (ver 17.11.1.3 na pág. 282)

Ficheiros de Dados
Nesta janela, pode configurar definições para registo de estatísticas sobre o funcionamento da aplicação (ver 17.3.1 na pág. 249) e especificar o tempo durante o qual os ficheiros são armazenados na Cópia de Segurança (ver 17.1.2 na pág. 242) e na Quarentena (ver 17.2.2 na pág. 245).
Definições de Rede
Nesta janela pode editar a lista de portas que o Kaspersky Anti-Virus usa para verificação (ver 17.7 na pág. 267) e activar/desactivar verificação de ligações SSL (ver 17.8 na pág. 269)

20.1.3. Configurar definições específicas

Quando administra o Kaspersky Anti-Virus através do Kaspersky Administration Kit, pode activar/desactivar a interactividade e editar a informação sobre o Suporte Técnico. Para o fazer:

1. Abra a janela de propriedades para o computador cliente no separador **Aplicações** (ver Figura 107). Seleccione o **Kaspersky Anti-Virus 6.0 para Windows Workstations** e clique no botão **Propriedades**. Como resultado, abrir-se-á uma janela de definições da aplicação.
2. Aceda ao separador **Definições** (ver Figura 108). Seleccione **Serviço** a partir do menu suspenso na parte superior da janela.

No separador **Serviço** na janela **Aparência**, pode activar/desactivar a interactividade do Kaspersky Anti-Virus num computador remoto: a apresentação do ícone do Kaspersky Anti-Virus na bandeja do sistema, a emissão de notificações sobre eventos ocorridos na aplicação (por exemplo, a detecção de um objecto perigoso).

Se a opção ☑ **Activar interacção com a interface** estiver assinalada, um utilizador que estiver a trabalhar num computador remoto verá o ícone e mensagens de pop-up do Anti-Virus e terá a capacidade para tomar decisões sobre os passos subsequentes a tomar nas janelas de notificação em relação a eventos que ocorram. Para desactivar a interactividade da aplicação, desmarque a caixa de selecção.

No separador **Informação de suporte personalizada,** na janela que se abre quando clica no botão **Definições**, pode editar a informação sobre o suporte técnico do utilizador, que é fornecida na secção **Serviço** do item **Suporte** do Kaspersky Anti-Virus (ver Figura 97).

Para alterar a informação no campo superior, introduza o texto actual sobre o suporte fornecido. No campo que surge por baixo, pode editar as hiperligações que são apresentadas na caixa **Suporte Técnico Online**, que se abre quando selecciona **Suporte** na secção **Serviço**.

Você pode editar a lista de origens, utilizando os botões **Adicionar**, **Editar** e **Apagar**. O Kaspersky Anti-Virus irá adicionar um novo link ao topo da lista. Para alterar a ordem dos links na lista, use os botões **Mover cima**/**Mover baixo**.

Se a janela não contiver nenhum dado, a informação predefinida sobre o suporte técnico não está sujeita a edição.

20.2. Gerir tarefas

Esta secção lista informação sobre como gerir tarefas para o Kaspersky Anti-Virus 6.0 para Windows Workstations. Para mais informação sobre o conceito de gestão de tarefas através do Kaspersky Administration Kit 6.0, veja o Guia do Administrador para o programa.

Quando a aplicação é instalada, é criado um conjunto de tarefas de sistema para cada computador. Esta lista (ver Figura 110) inclui tarefas de protecção em tempo real (Anti-vírus de Ficheiros, Anti-vírus de Internet, Anti-vírus de E-mail, Defesa Pró-activa, Anti-Spy e Anti-Hacker), tarefas de verificação de vírus (O Meu Computador, Objectos de Inicialização, Áreas Críticas) e tarefas de actualização (actualizações de assinaturas de ameaças e dos módulos da aplicação e reversão de actualizações).

> Você pode iniciar tarefas de sistema e configurar definições e agendamentos para as mesmas, mas as mesmas não podem ser apagadas.

Para além disso, você pode criar as suas próprias tarefas, tais como verificações de vírus, actualizações da aplicação, reversão de actualizações, assim como tarefas de instalação de chaves de licença (ver 20.2.2 na pág. 318).

Para ver uma lista das tarefas criadas para um computador cliente:

1. Seleccione a pasta do grupo que contém o computador cliente na pasta **Grupos** (ver Figura 106).

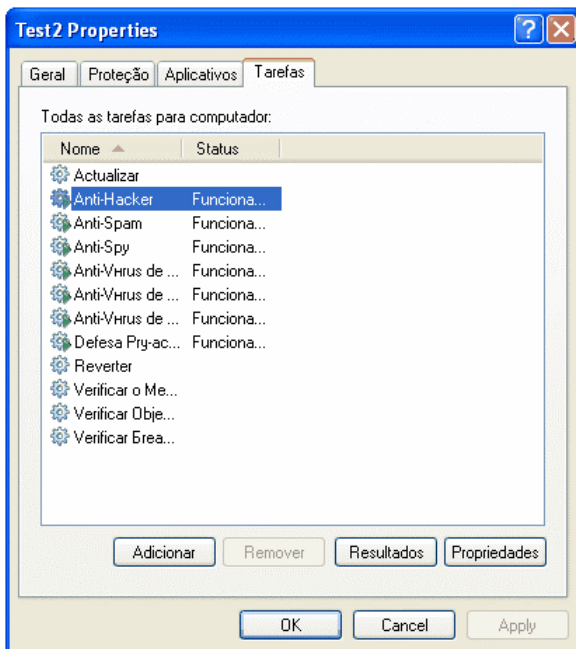



Figura 110. Lista de tarefas das aplicações

2. Na janela que se abre, seleccione o computador para o qual você pretende ver uma lista de tarefas locais. Use o comando **Tarefas** no menu de contexto ou o mesmo comando no menu **Acções**. De seguida, na janela principal abrir-se-á uma janela com as propriedades do computador cliente.
3. O separador **Tarefas** (ver Figura 110) apresenta uma lista completa das tarefas criadas para aquele computador cliente.

20.2.1. Iniciar e parar tarefas

> As tarefas são iniciadas no computador cliente apenas se a aplicação correspondente estiver a funcionar (ver 20.1.1 na pág. 312. Se a aplicação estiver parada, todas as tarefas serão terminadas.

As tarefas são iniciadas e pausadas automaticamente, de acordo com um agendamento, ou manualmente, utilizando os comandos a partir do menu de

contexto e a partir da janela Ver Definições da Tarefa. Também pode pausar tarefas e retomá-las.

Para iniciar/parar/pausar/retomar uma tarefa manualmente:

Seleccione a tarefa necessária (grupo ou global) a partir da janela de resultados, abra o menu de contexto e seleccione **Iniciar/Parar/Pausar/Retomar** ou use os mesmos comandos no menu **Acções**.

Pode iniciar as mesmas operações para todos os tipos de tarefas a partir da janela de definições da tarefa no separador **Geral** (ver Figura 111), utilizando os mesmos botões de comando.

20.2.2. Criar tarefas

Ao trabalhar com a aplicação através do Kaspersky Administration Kit, você pode criar:

- Tarefas locais, configuradas para computadores individuais
- Tarefas de grupo, configuradas para computadores unidos num grupo da rede
- Tarefas globais, configuradas para qualquer conjunto de computadores de qualquer grupo da rede

Você pode alterar as definições de tarefas, monitorizar o seu desempenho, copiar e mover tarefas de um grupo para outro e também apagá-las, utilizando os comandos padrão **Copiar/Colar**, **Cortar/Colar** e **Apagar** a partir do menu de contexto ou os mesmos comandos a partir do menu **Acções**.

20.2.2.1. Criar tarefas locais

Para criar uma tarefa local, siga os seguintes passos:

1. Abra a janela de propriedades do cliente local no separador **Tarefas** (ver Figura 110).
2. Use o botão **Adicionar** para adicionar uma nova tarefa local. Iniciar-se-á um assistente de criação de tarefas que consiste numa série de janelas ou passos e você pode navegar entre eles utilizando os botões **Anterior** e **Seguinte**. Você completa o assistente, clivando em **Concluir**. O botão **Cancelar** irá parar o processo em qualquer ponto.

Passo 1. Introduzir dados gerais na tarefas

A primeira janela principal é introdutória: aqui deve especificar o nome da tarefa (o campo **Nome**).

Passo 2. Seleccionar uma aplicação e tipo de tarefa

Neste passo, deve especificar a aplicação para a qual está a ser criada a tarefa (Kaspersky Anti-Virus 6.0 para Windows Workstations). Também tem de seleccionar o tipo de tarefa. As tarefas possíveis para o Kaspersky Anti-Virus 6.0 são:

- *Verificação de vírus* – verifica a existência de vírus nas áreas especificadas pelo utilizador
- *Actualização* – recolhe e aplica pacotes de actualização para o programa
- *Reversão de Actualização* – reverte a última actualização do programa que foi efectuada
- *Instalação de Chave de Licença* – adicionar uma nova chave de licença para utilizar a aplicação

Passo 3. Configurar definições para o tipo de tarefa seleccionado

Dependendo do tipo de tarefa seleccionado no passo anterior, os conteúdos das janelas que se seguem podem variar:

VERIFICAÇÃO DE VÍRUS

A janela de configuração da tarefa de verificação de vírus requer que você especifique a acção que o Kaspersky Anti-Virus irá tomar, quando detectar um objecto perigoso (ver 14.4.4 na pág. 214). Também deve criar uma lista de objectos a verificar (ver 14.2 na pág. 205).

ACTUALIZAÇÃO

Para as tarefas de actualização das assinaturas de ameaças e dos módulos da aplicação, tem de especificar a origem que será utilizada para transferir as actualizações (ver 16.4.1 na pág. 228). Por defeito, a origem de actualização é o servidor de actualização do Kaspersky Administration Kit.

REVERSÃO DE ACTUALIZAÇÃO

Não existem definições específicas para reverter a actualização mais recente.

INSTALAR CHAVE DE LICENÇA

Para as tarefas de instalação de chaves de licença, especifique o caminho para o ficheiro da chave com o botão **Procurar**. Para tornar uma chave adicionada numa reserva, assinale a opção ☑ **Adicionar como chave de reserva**. A chave de reserva tornar-se-á activa quando a actual chave de licença expirar.

O campo por baixo apresenta informação sobre a licença adicionada (número de licença, tipo e a data de validade).

Passo 4. Seleccionar um perfil de utilizador

Neste passo, é-lhe pedido que configure as tarefas para se iniciarem com uma conta de utilizador com privilégios suficientes para aceder ao objecto a ser verificado ou à origem de actualização (para mais detalhes, ver 6.4 na pág. 87).

Passo 5. Configurar um agendamento

Após configurar as definições da tarefa, ser-lhe-á pedido que configure um agendamento automático da tarefa.

Para o fazer, seleccione a frequência para a execução da tarefa a partir do menu suspenso e ajuste as definições de agendamento na parte inferior da janela.

Passo 6. Concluir a criação de uma tarefa

A última janela do assistente irá informá-lo de que criou uma tarefa com sucesso.

20.2.2.2. Criar tarefas de grupo

Para criar uma tarefa de grupo, siga os seguintes passos:

1. Seleccione o grupo para o qual pretende criar uma tarefa, a partir da árvore da consola.
2. Seleccione a respectiva pasta de **Tarefas** (ver Figura 106), abra o menu de contexto e seleccione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Acções**. O assistente de criação da tarefa irá então iniciar-se, da mesma forma que o assistente para criar uma tarefa local (para mais informações, ver 20.2.2.1 na pág. 318). Siga as suas instruções.

Quando o assistente estiver concluído, a tarefa será adicionada à pasta **Tarefas** daquele grupo e de todos os grupos por baixo do mesmo e estará visível na janela de resultados.

20.2.2.3. Criar tarefas globais

Para criar uma tarefa global, siga os seguintes passos:

1. Seleccione o nódulo **Tarefas globais** na árvore da consola (ver Figura 106), abra o menu de contexto e seleccione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Acções**.
2. O assistente de criação da tarefa irá então iniciar-se, da mesma forma que o assistente para criar uma tarefa local (para mais informação, ver 20.2.2.1 na pág. 318). A excepção é que existe uma etapa para criar uma lista de computadores cliente a partir da rede, para os quais a tarefa global está a ser criada.
3. Seleccione na rede os computadores que irão executar a tarefa. Pode seleccionar computadores de pastas múltiplas ou seleccionar uma pasta inteira (para mais detalhes, veja o Guia do Administrador para o Kaspersky Administration Kit 6.0).

> As tarefas globais apenas são efectuadas num conjunto seleccionado de computadores. Se forem adicionados novos computadores cliente a um grupo com computadores para os quais foi criada uma tarefa de instalação remota, esta tarefa não será executada para esses novos computadores. Tem de criar uma nova tarefa ou fazer as alterações correspondentes nas definições da tarefa existente.

Quando o assistente estiver concluído, será adicionada uma tarefa global ao nódulo **Tarefas globais** da árvore da consola e estará visível na janela de resultados.

20.2.3. Configurar definições específicas de tarefas

Para ver e alterar as definições de tarefas do computador cliente:

1. Abra a janela de propriedades para o computador cliente no separador **Tarefas** (ver Figura 110).
2. Seleccione a tarefa na lista e clique no botão **Propriedades**. Como resultado, abrir-se-á uma janela de definições da tarefa (ver Figura 111).

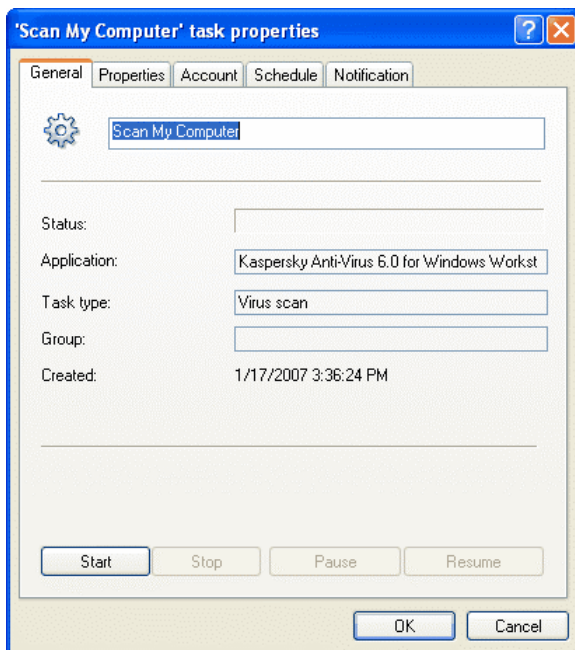



Figura 111. Configurar definições de tarefa

Todos os separadores, com excepção do separador **Definições,** são separadores padrão para o Kaspersky Administration Kit 6.0. Estes são abordados em maior detalhe no Manual de Utilização do Administrador. O separador **Definições** contém definições específicas para o Kaspersky Anti-Virus. Os conteúdos deste separador variam, dependendo do tipo de tarefa seleccionada.

A configuração das definições de tarefa do programa através da interface do Kaspersky Administration Kit é semelhante à configuração através da interface local do Kaspersky Anti-Virus, com a excepção das definições que são configuradas individualmente para cada utilizador, tais como as listas branca e negra do Anti-Spam. Veja o Capítulo 7 – Capítulo 16 on pp. 92 – 224 deste Manual do Utilizador para uma descrição mais aprofundada da configuração de definições de tarefa.

Se tiver sido criada uma política para a aplicação (ver 20.3 na pág. 323) que impede que algumas definições sejam reconfiguradas, estas não serão editáveis ao configurar as tarefas.

20.3. Gerir políticas

A configuração de políticas permite-lhe aplicar definições universais da aplicação e das tarefas aos computadores cliente que pertencem a um único grupo da rede.

Esta secção inclui informação sobre a criação e configuração de políticas do Kaspersky Anti-Virus 6.0 para Windows Workstations. Para mais informação sobre o conceito de gestão de tarefas através do Kaspersky Administration Kit 6.0, veja o Guia do Administrador para o programa.

20.3.1. Criar políticas

Para criar uma política para o Kaspersky Anti-Virus, siga os seguintes passos:

1. Seleccione o grupo de computadores para os quais precisa de criar uma política (ver Figura 106) na pasta **Grupos**.
2. Seleccione a pasta **Políticas** que pertence ao grupo seleccionado, abra o menu de contexto e use o comando **Criar→Política**. Aparecerá uma janela Criar Nova Política.

As políticas são criadas num assistente de janelas e consiste numa série de janelas ou passos e você pode navegar entre eles utilizando os botões **Anterior** e **Seguinte**. Você completa o assistente, clivando em **Concluir**. O botão **Cancelar** irá parar o processo em qualquer ponto.

Durante cada passo da criação de uma política, as definições inseridas podem ser bloqueadas com o botão 🔓. Se o cadeado do botão estiver fechado, no futuro os valores atribuídos pela política criada serão utilizados quando usar a política nos computadores cliente.

Passo 1. Introduzir dados gerais na política

O primeiro passo do assistente é introdutório. Na primeira janela do assistente deve especificar o nome da política (o campo **Nome**). Na segunda janela, seleccione o **Kaspersky Anti-Virus 6.0 para Windows Workstations** a partir do menu suspenso **Nome da aplicação**. Se quiser que as definições de política entrem imediatamente em efeito depois de a ter criado, assinale a opção **Tornar a política activa**.

Passo 2. Seleccionar o estado de uma política

Esta janela pedir-lhe-á para especificar o estado da política. Para o fazer, desloque o indicador para a posição desejada: política active ou política inactiva.

Podem ser criadas várias políticas num grupo para uma aplicação, mas apenas uma delas pode ser a política actual (activa).

Passo 3. Seleccionar e configurar as componentes de protecção

Nesta etapa, você pode activar/desactivar e configurar as componentes de protecção que serão utilizadas na política.

Por defeito, todas as componentes de protecção estão activadas. Para desactivar uma componente, desmarque a caixa junto ao nome da mesma. Para ajustar as definições de protecção ou para configurar o Anti-vírus de Ficheiros, seleccione-os na lista e clique no botão **Definições**.

Passo 4. Configurar as definições de verificação de vírus

Nesta etapa, pode configurar as definições que serão usadas pelas tarefas de verificação de vírus.

Na secção **Nível de segurança**, seleccione um dos três níveis de segurança pré-configurados (ver 14.4.1 na pág. 209). Para ajustar o nível seleccionado, clique no botão **Definições**. Para restaurar as definições do nível **Recomendado**, use o botão **Predefinições**.

Na secção **Acções**, especifique a acção que o Anti-vírus deve tomar quando for detectado um objecto perigoso (ver 14.4.4 na pág. 214).

Passo 5. Configurar definições de actualização

Nesta janela, configure as definições para a função de distribuição de actualizações do Kaspersky Anti-Virus.

Na secção **Definições de actualização**, especifique o que está a ser actualizado (ver 16.4.2 na pág. 231). Na janela que se abre quando clica no botão **Definições**, atribua as definições locais de rede (ver 16.4.3 na pág. 233) e especifique a origem de actualização (ver 16.4.1 na pág.228).

Na secção **Acção após Actualização**, active/desactive a verificação da Quarentena após a recepção de um novo pacote de actualização (ver 16.4.4 na pág. 235).

Passo 6. Implementação da política

Nesta etapa, seleccione um método para a implementação da política nos computadores cliente do grupo (para mais detalhes, consulte o Guia do Administrador do Kaspersky Administration Kit 6.0).

Passo 7. Concluir a criação de uma política

A janela final do assistente informa-o de que criou uma política com sucesso.

Assim que o assistente estiver concluído, a política do Kaspersky Anti-Virus será adicionada à pasta **Políticas** (ver Figura 106) para o grupo correspondente e estará visível na janela de resultados.

Pode editar as definições da política criada e definir restrições à alteração das suas definições, utilizando o botão para cada grupo de definições. Se essas definições estiverem bloqueadas, um utilizador no computador cliente não poderá alterar as definições. A política será aplicada aos computadores cliente na primeira vez que os clientes sincronizarem com o servidor.

Pode copiar ou mover políticas de um grupo para outro e apagá-las, utilizando os comandos padrão **Copiar/Colar**, **Cortar/Colar** e **Apagar** a partir do menu de contexto ou os mesmos comandos a partir do menu **Acções**.

20.3.2. Ver e editar definições da política

Na etapa de edição, pode alterar a política e bloquear a alteração das definições em políticas de grupos aninhados e em definições da aplicação e de tarefas.

Para ver e editar as definições de políticas:

1. Seleccione o grupo de computadores para o qual precisa de editar as definições, a partir da árvore da consola na pasta **Grupos**.
2. Seleccione uma pasta **Políticas** que pertença àquele grupo (ver Figura 106). Quando o fizer, a janela de resultados apresentará todas as políticas criadas para o grupo.
3. Seleccione a política de que precisa a partir da lista de políticas do **Kaspersky Anti-Virus 6.0 para Windows Workstations** (o nome da aplicação é especificado no campo **Aplicação**).
4. Seleccione o comando **Propriedades** a partir do menu de contexto para a política seleccionada. Abrir-se-á uma janela de definições da política para a aplicação, contento vários separadores (ver Figura 112).

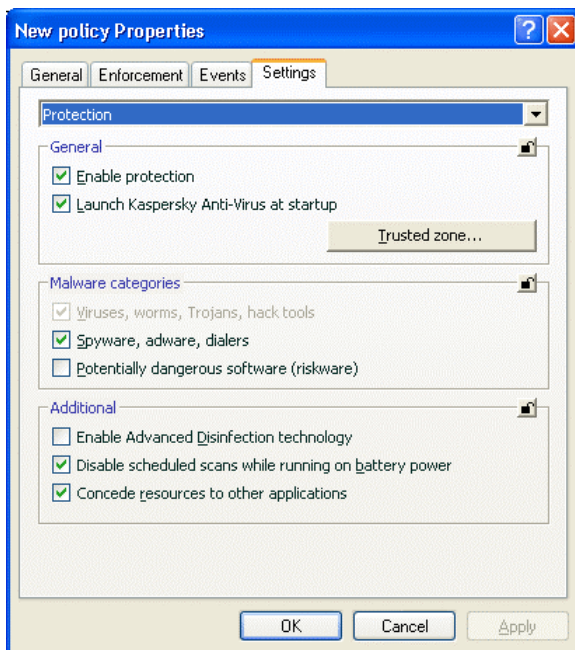



Figura 112. Configurar definições de política

Todos os separadores, com excepção do separador **Definições,** são separadores padrão para o Kaspersky Administration Kit 6.0. (para mais detalhes, veja o Manual do Administrador para o programa).

O separador **Definições** contém as definições da política para o Kaspersky Anti-Virus 6.0. As definições da política incluem as definições do programa (ver 20.1.2 na pág. 313) e as definições de tarefas (ver 20.1.3 na pág. 315).

Para configurar as definições, seleccione o valor necessário do menu suspenso na parte superior da janela e configure as definições.

CAPÍTULO 21. PERGUNTAS FREQUENTES

Este capítulo é dedicado às questões mais frequentes colocadas pelos utilizadores em relação à instalação, configuração e funcionamento do Kaspersky Anti-virus para Windows Workstations; aqui tentaremos responder, em detalhe, a essas perguntas.

Pergunta: *É possível utilizar o Kaspersky Anti-virus 6.0 para Windows Workstations com softwares de anti-vírus de outros fabricantes?*

Não. Para evitar conflitos de software, recomendamos que desinstale os softwares de anti-vírus de outros fabricantes antes de instalar o Kaspersky Anti-virus para Windows Workstations.

Pergunta: *O Kaspersky Anti-virus para Windows Workstations não revê ficheiros que já foram verificados anteriormente. Porquê?*

Isto é verdade. O Kaspersky Anti-virus para Windows Workstations não revê ficheiros que não foram modificados desde a última verificação.

Isso tornou-se possível devido às novas tecnologias iChecker e iStreams. A tecnologia é implementada no programa, utilizando uma base de dados de somas de verificação de ficheiros e armazenamento de somas de verificação de ficheiros em fluxos de dados alternados em volumes NTFS.

Pergunta: *Porque é que preciso do ficheiro da chave de licença? O Kaspersky Anti-virus para Windows Workstations funcionará sem esse ficheiro?*

O Kaspersky Anti-virus para Windows Workstations funcionará sem uma chave de licença, mas você não será capaz de aceder ao Actualizador e Suporte Técnico.

Se ainda não decidiu se vai comprar o Kaspersky Anti-virus para Windows Workstations, podemos lhe fornecer uma chave de avaliação que funcionará durante duas semanas ou um mês. Após decorrido esse tempo, a chave expirará.

Pergunta: *Após a instalação do Kaspersky Anti-virus para Windows Workstations, o sistema operativo começou a "comportar-se" de forma estranha ("ecrã azul (BSOD)", reinicialização frequente, etc.). O que devo fazer?*

Embora raro, é possível que o Kaspersky Anti-virus para Windows Workstations e outro software instalado no seu computador estejam em conflito.

Para restaurar a funcionalidade do seu sistema operativo, faça o seguinte:

1. Prima a tecla F8 assim que o computador começar a carregar até que o menu de inicialização seja apresentado.
2. Seleccione o item **Modo de Segurança** (Safe Mode) e carregue o sistema operativo.
3. Abra o Kaspersky Anti-virus para Windows Workstations.
4. Utilize a ligação Definições na janela principal e seleccione a secção **Protecção** na janela de definições do programa.
5. Desmarque a opção **Iniciar o Kaspersky Anti-Virus 6.0 com a inicialização do sistema** e clique em **OK.**
6. Volte a carregar o sistema operativo no modo normal.

Depois disto, contacte o Serviço de Suporte Técnico através do site da Kaspersky Lab (**Serviços → Suporte Técnico)**. Descreva detalhadamente o problema e as circunstâncias em que ele aconteceu.

Certifique-se de que anexa à sua questão um ficheiro com a descarga completa do sistema operativo Microsoft Windows. Para criar este ficheiro, faça o seguinte:

1. Clique com o botão direito do rato em **O Meu Computador** (My Computer) e seleccione o item **Propriedades** (Properties) no menu de atalho que se abre.
2. Seleccione o separador **Avançadas** (Advanced) na janela **Propriedades do Sistema** (System Properties) e depois prima o botão **Definições** (Settings) na secção **Inicialização e Recuperação** (Startup and Recovery).
3. Seleccione a opção **Informação completa de estado da memória** (Complete memory dump) através da lista suspensa existente na secção **Escrever informações de depuração** (Write debugging information) da janela **Inicialização e Recuperação** (Startup and Recovery).
4. Por definição, o ficheiro de descarga será guardado na pasta do sistema como *memory.dmp*. Você pode alterar a pasta de armazenamento de ficheiros de descarga editando o nome da pasta no campo correspondente.
5. Reproduza o problema relacionado com o funcionamento do Kaspersky Anti-virus para Windows Workstations.
6. Certifique-se que o ficheiro de descarga completa de memória foi guardado com sucesso.

APÊNDICE A. INFORMAÇÃO DE REFERÊNCIA

Este apêndice contém materiais de referência sobre os formatos de ficheiro e as máscaras de extensão utilizadas pelas definições do Kaspersky Anti-Virus e também é fornecida informação sobre as definições no ficheiro setup.ini, que é usado ao instalar o programa em modo oculto.

A.1. Lista de ficheiros verificados por extensão

Se seleccionou a opção **Programas e documentos (por extensão)** como a opção de verificação do Anti-vírus de Ficheiros ou da tarefa de verificação de vírus, os ficheiros com as extensões abaixo listadas serão analisados, em profundidade, quanto à existência de vírus. Estes tipos de ficheiros também são verificados pelo Anti-vírus de E-mail se for activada a verificação de anexos de e-mails:

com – ficheiro executável para um programa

exe – ficheiro executável ou arquivo auto-extraível

sys – controlador do sistema

prg – texto de programa para o dBase, Clipper ou Microsoft Visual FoxPro ou um programa para criação de ficheiros .wav

bin - ficheiro binário

bat - ficheiro batch

cmd - ficheiro de comandos para o Microsoft Windows NT (semelhante a um ficheiro .bat para o DOS), OS/2.

dpl - biblioteca compactada do Borland Delphi

dll - biblioteca de ligação dinâmica

scr - ecrã de entrada do Microsoft Windows

cpl - módulo do painel de controlo do Microsoft Windows

ocx - objecto OLE (Ligação e Incorporação de Objectos) da Microsoft

tsp - programa executado em modo de tempos fraccionados

drv - controlador de dispositivo

vxd - controlador de dispositivo virtual do Microsoft Windows

pif - ficheiro de informações de programa

lnk - ficheiro de ligação do Microsoft Windows

reg - ficheiro de chave de registo do sistema do Microsoft Windows

ini - ficheiro de inicialização

cla - classe de Java

vbs - script de Visual Basic

vbe - extensão da BIOS de vídeo

js, jse - texto fonte de JavaScript

htm - documento de hipertexto

htt - cabeçalho de hipertexto do Microsoft Windows

hta - programa de hipertexto para o Microsoft Internet Explorer

asp - script de Active Server Pages (Páginas de Servidor Activas)

chm - ficheiro HTML compilado

pht - HTML com scripts PHP incorporados

php - script incorporado em ficheiros HTML

wsh - ficheiro do script anfitrião do Microsoft Windows

wsf - script do Microsoft Windows

the - plano de fundo da área de trabalho do Microsoft Windows 95

hlp - ficheiro de ajuda do Windows

eml - ficheiro de e-mail do Microsoft Outlook Express

nws - ficheiro de e-mail novo do Microsoft Outlook Express

msg - ficheiro de e-mail do Microsoft Mail

plg - e-mail

mbx - extensão para os e-mails guardados do Microsoft Office Outlook

*doc** – um documento do Microsoft Word, tal como: *doc* – um documento do Microsoft Word, *docx* – um documento do Microsoft Word 2007 com suporte XML, *docm* – um documento do Microsoft Word 2007 com suporte de Macros

*dot** – um modelo de documento do Microsoft Word, tal como: *dot* – um modelo de documento do Microsoft Word, *dotx* – um modelo de documento do Microsoft Word 2007, *dotm* – modelo de documento do Microsoft Word 2007 com suporte de Macros

fpm - programa de base de dados, ficheiro de início para o Microsoft Visual FoxPro

rtf - documento em Formato de Texto Rico

shs - manipulador de objecto de recorte do Shell

dwg - base de dados de desenhos do AutoCAD

msi - pacote de instalação do Microsoft Windows

otm - projecto VBA para o Microsoft Office Outlook

pdf - documento do Adobe Acrobat

swf - ficheiro do Shockwave Flash

jpg, jpeg, png - formato gráfico de imagens comprimidas

emf - formato de metaficheiro avançado. A próxima geração dos metaficheiros do SO Microsoft Windows. Os ficheiros EMF são suportados pelo Microsoft Windows 16-bit.

ico - ficheiro de ícone

ov? - ficheiros executáveis do MS DOC

*xl** – documentos e ficheiros do Microsoft Office Excel, tais como: *xla* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento xlsx – uma folha de trabalho do Microsoft Excel 2007, *xltm* – um folha de trabalho do Microsoft Excel 2007 workbook suporte de Macros, *xlsb* – um formato (não-XML) em binário do Microsoft Excel 2007, *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de Macros, *xlam* – uma extensão do Microsoft Excel 2007 com suporte de Macros.

*pp** – documentos e ficheiros do Microsoft Office PowerPoint, tais como: *pps* - diapositivo do Microsoft Office PowerPoint, *ppt* - apresentação, *pptx* – uma apresentação do Microsoft PowerPoint 2007, *pptm* – uma apresentação do Microsoft PowerPoint 2007 com suporte de Macros, *potx* – um modelo de apresentação do Microsoft PowerPoint 2007, *potm* – um modelo de apresentação do Microsoft PowerPoint 2007 com suporte de Macros, *ppsx* – um apresentação de diapositivos do Microsoft PowerPoint 2007, *ppsm* – uma apresentação de diapositivos do Microsoft PowerPoint 2007 com suporte de Macros, *ppam* – uma extensão do Microsoft PowerPoint 2007 com suporte de Macros.

*md** – documentos e ficheiros do Microsoft Office Access, tais como: *mda* - grupo de trabalho do Microsoft Office Access, *mdb* - base de dados, etc.

sldx – um diapositivo do Microsoft PowerPoint 2007.

sldm – um diapositivo do Microsoft PowerPoint 2007 slcom suporte de Macros.

thmx – um tema do Microsoft Office 2007.

Lembre-se que o verdadeiro formato de um ficheiro pode não corresponder ao formato indicado na extensão do ficheiro.

A.2. Máscaras de exclusão de ficheiros possíveis

Vejamos alguns exemplos de máscaras possíveis que você poderá utilizar ao criar listas de exclusão de ficheiros:

- Máscara sem caminhos de ficheiro:
  - ***.exe** – todos os ficheiros com a extensão*.exe*
  - ***.ex?** – todos os ficheiros com a extensão .ex?, onde ? pode representar qualquer caractere único
  - **teste** – todos os ficheiros com o nome teste
- Máscaras com caminhos de ficheiro absolutos:
  - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** – todos os ficheiros incluídos na pasta *C:\dir*
  - **C:\dir*.exe** – todos os ficheiros com a extensão *.exe* incluídos na pasta *C:\dir*
  - **C:\dir*.ex?** – todos os ficheiros com a extensão .ex? incluídos na pasta C:\dir\, onde ? pode representar qualquer caractere único
  - **C:\dir\teste** – apenas o ficheiro *C:\dir\teste*
  - Se não pretende que o programa verifique os ficheiros incluídos nas subpastas desta pasta, desmarque a opção **Incluir subpastas** quando criar a máscara.
- Máscaras com caminhos de ficheiro relativos:
  - **dir*.*** ou **dir*** ou **dir** – todos os ficheiros em todas as pastas dir\
  - **dir\teste** – todos os ficheiros teste incluídos nas pastas dir\
  - **dir*.exe** – todos os ficheiros com a extensão .exe incluídos em todas as pastas dir\
  - **dir*.ex?** – todos os ficheiros com a extensão .ex? incluídos em todas as pastas C:\dir\ , onde ? pode representar qualquer caractere único

- Se não pretende que o programa verifique os ficheiros incluídos nas subpastas desta pasta, desmarque a opção **Incluir subpastas** quando criar a máscara.

Dica:

As máscaras de exclusão *.* e * apenas podem ser utilizadas se você atribuir a uma ameaça excluída um veredicto, de acordo com a Enciclopédia de Vírus. Caso contrário, a ameaça especificada não será detectada em nenhum dos objectos. Se utilizar estas máscaras sem seleccionar um veredicto, basicamente isso significa desactivar a monitorização.

Nós também não recomendamos que seleccione uma unidade virtual como uma exclusão que foi criada com base num directório do sistema de ficheiros, utilizando o comando subst. Não há razão para o fazer, uma vez que durante a verificação, o programa considera essa unidade virtual como sendo uma pasta e, por conseguinte, verifica-a.

A.3. Possíveis máscaras de exclusão de ameaças

Quando adicionar, enquanto exclusões, as ameaças com um determinado veredicto da Enciclopédia de Vírus, você pode especificar:

- O nome completo da ameaça tal como aparece listado na Enciclopédia de Vírus presente em www.viruslist.com (por exemplo, **não é vírus:RiskWare.RemoteAdmin.RA.311 ou Flooder.Win32.Fuxx);**
- o nome da ameaça através da máscara. Por exemplo:
    - **não é vírus* –** exclui da verificação programas legais, mas potencialmente perigosos, assim como programas de brincadeiras (joke programs).
    - ***Riskware.* –** exclui da verificação o riskware (software potencialmente perigoso).
    - ***RemoteAdmin.*** – exclui da verificação todos os programas de administração remota.

A.4. Resumo das definições no ficheiro *setup.ini*

O ficheiro *setup.ini*, localizado na pasta de instalação do Kaspersky Anti-Virus, é utilizado ao instalar o programa no modo não interactivo a partir da linha de comandos (ver 3.3 na pág. 48) ou utilizando o Editor de Objectos de Política de Grupo (ver 3.4 na pág.49). O ficheiro contém as seguintes definições:

[Setup] – definições gerais para a instalação do programa.

InstallDir=<caminho para a pasta de instalação do programa>.

Reboot=sim|não – define se o computador deve ou não ser reiniciado depois do programa ser instalado (por defeito, não se reinicia).

SelfProtection=sim|não – define se o Kaspersky Anti-Virus deve ou não activar a Auto-defesa durante a instalação (por defeito, está activada).

[Components] – selecciona as componentes a instalar. Se este grupo não contiver nenhum item, serão todas instaladas.

FileMonitor=sim|não – instala o Anti-vírus de Ficheiros

MailMonitor=sim|não – instala o Anti-vírus de E-mail

WebMonitor=sim|não – instala o Anti-vírus de Internet

ProactiveDefence=sim|não – instala a Defesa Pró-activa

AntiSpy=sim|não – instala o Anti-Spy

AntiHacker=sim|não – instala o Anti-Hacker

AntiSpam=sim|não – instala o Anti-Spam

[Tasks] – activa as tarefas do Kaspersky Anti-Virus. Se não for especificada nenhuma tarefa, após a instalação todas as tarefas funcionarão. Se tiver especificado algumas tarefas, todas as tarefas que não estiverem listadas serão desactivadas.

ScanMyComputer=sim|não – tarefa para a verificação completa do computador

ScanStartup=sim|não – tarefa para a verificação de objectos de inicialização

ScanCritical=sim|não – tarefa para a verificação de áreas críticas

Updater=sim|não – tarefa para a actualização de assinaturas de ameaças e módulos do programa

Em vez do valor **sim**, pode utilizar os valores **1**, **on**, **activar** ou **activado** e em vez de **não** pode usar – **0**, **off**, **desactivar** ou **desactivado**.

APÊNDICE B. KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab tornou-se num líder reconhecido nas tecnologias de segurança de informação. Produz uma ampla gama de software para segurança de dados e fornece soluções de alta performance e abrangentes para proteger computadores e redes em relação a todos os tipos de programas maliciosos, mensagens de e-mail não-solicitadas e indesejadas e ataques de hackers.

A Kaspersky Lab é uma empresa internacional. Centralizada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, EUA (Califórnia), Benelux, China, Polónia, e Roménia. Um novo departamento da empresa, o Centro Europeu de Pesquisa Anti-vírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 450 especialistas, cada um versado em tecnologias anti-vírus, em que 10 deles têm graduações M.B.A., 16 têm doutoramentos e especialistas membros da Computer Anti-virus Researchers Organization (CARO).

A Kaspersky Lab oferece as melhores soluções de segurança, baseadas na sua experiência única e conhecimento, obtidos ao longo de mais de 14 anos a combater vírus de computador. Uma análise detalhada das actividades do vírus de computador permite que a empresa forneça uma protecção global em relação a ameaças correntes e futuras. A resistência a ataques futuros é a política de base implementada em todos os produtos da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente de muitos outros vendedores no fornecimento de uma cobertura anti-vírus extensiva tanto para utilizadores domésticos, como para empresas.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software de segurança. A Kaspersky Lab foi uma das primeiras companhias do seu género a desenvolver as melhores normas de defesa anti-vírus. O produto emblemático da empresa, o Kaspersky Anti-virus, permite a protecção total para todos os níveis da rede, incluindo estações, servidores, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão adequadas e intuitivas asseguram uma automação avançada para a protecção rápida contra vírus em toda a empresa. Muitos fabricantes conhecidos usam o núcleo do Kaspersky Anti-virus, incluindo a Nokia ICG (EUA), F-Secure (Finlândia), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, como a conformidade com as necessidades específicas da empresa.

A base de dados anti-vírus da Kaspersky Lab é actualizada a cada hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, que está disponível em várias línguas para satisfazer os seus clientes internacionais.

B.1. Outros produtos da Kaspersky Lab

News Agent da Kaspersky Lab

O News Agent (Agente de Notícias) é destinado à entrega, atempada, de notícias publicadas pela Kaspersky Lab, notificações sobre o estado actual da actividade de vírus e notícias recentes. O programa lê a lista de fontes de notícias disponíveis e o seu conteúdo a partir do servidor de notícias da Kaspersky Lab em intervalos especificados.

O News Agent permite aos utilizadores;

- See the current virus forecast in the system tray.
- Ver a previsão actual de vírus na bandeja do sistema.
- Subscrever e anular a subscrição de notícias.
- Recolher notícias de cada fonte de notícias seleccionada, no intervalo especificado e receber notificações sobre notícias recentes.
- Rever notícias nas fontes seleccionadas.
- Rever a lista de fontes e o seu estado.
- Abrir textos completos de artigos no seu navegador.

O News Agent é uma aplicação independente do Microsoft Windows, que pode ser usada sozinha ou em conjunto com várias soluções integradas oferecidas pela Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Este programa é um serviço livre fornecido aos visitantes da página de Internet da Kaspersky Lab. O serviço permite uma verificação eficiente e online de vírus no seu computador. O Kaspersky On-Line Scanner Kaspersky OnLine Scanner é executado directamente no navegador da Internet. Assim, os utilizadores recebem respostas rápidas a questões sobre infecções potenciais nos seus computadores. Ao utilizar o serviço, os visitantes podem:

- Excluir da verificação arquivos e bases de dados de e-mail.
- Seleccionar bases de dados padrão/alargadas para a verificação.

- Guardar um relatório sobre os resultados da verificação em formatos txt ou html.

Kaspersky® OnLine Scanner Pro

O programa é um serviço de assinatura acessível aos visitantes da página da Web da Kaspersky Lab. O serviço permite uma verificação eficiente e online de vírus no seu computador e desinfecta ficheiros perigosos. O Kaspersky OnLine Scanner Pro é executado directamente no navegador da Internet. Ao utilizar o serviço, os visitantes podem:

- Excluir da verificação arquivos e bases de dados de e-mail.
- Seleccionar bases de dados padrão/alargadas para a verificação.
- Guardar um relatório sobre os resultados da verificação em formatos txt ou html.

Kaspersky Anti-Virus® 7.0

O Kaspersky Anti-Virus 7.0 foi concebido para salvaguardar computadores pessoais contra software malicioso, com combinação optimizada de métodos convencionais de protecção anti-vírus e de novas tecnologias pró-activas.

O programa permite verificações complexas de vírus, incluindo:

- Verificação anti-vírus do tráfego de e-mail ao nível dos protocolos de transmissão de dados (POP3, IMAP e NNTP para mensagens de entrada e SMTP para mensagens de saída), independentemente do cliente e-mail a ser usado, assim como a desinfecção de bases de dados de e-mail.
- Verificação anti-vírus, em tempo real, do tráfego de Internet transferido por HTTP.
- Verificação anti-vírus em ficheiros individuais, pastas ou unidades. Além disto, pode ser usada uma tarefa predefinida de verificação para iniciar a verificação anti-vírus, exclusivamente, para áreas críticas do sistema operativo e objectos de inicialização do Microsoft Windows.

A protecção pró-activa oferece as seguintes funções:

- **Controlo das alterações ao sistema de ficheiros**. O programa permite que os utilizadores criem uma lista de aplicações, que controlará numa base de componentes. Ajuda a proteger a integridade da aplicação face à influência de software malicioso.
- **Monitorização de processos na memória de acesso aleatório**. O Kaspersky Anti-vírus 7.0 notifica, atempadamente, os utilizadores quando

detecta processos perigosos, suspeitos ou escondidos ou em caso de ocorrerem alterações não-autorizadas em processos activos.

- **Monitorizar alterações no registo do Sistema Operativo** devido ao controlo interno do registo do sistema.
- **Monitorização de Processos Ocultos** ajuda a proteger de código malicioso escondido no sistema operativo através de tecnologias de processos ocultos (rootkit).
- **Analisador Heurístico**. Ao analisar um programa, o analisador simula a sua execução e regista todas as actividades suspeitas, tais como a abertura ou escrita num ficheiro, intercepção de vectores interrompidos, etc. É tomada uma decisão com base neste procedimento relativamente à possível infecção do programa com um vírus. A simulação ocorre num ambiente virtual isolado que protege o computador da infecção.
- **Restauro do sistema** após ataques de software malicioso, registando todas as alterações no registo e no sistema de ficheiros do computador, com a oportunidade para efectuar recuperações a pedido do utilizador.

Kaspersky® Internet Security 7.0

O Kaspersky® Internet Security 7.0 é uma solução integrada para a protecção dos seus computadores pessoais em relação às principais ameaças relacionadas com a informação, ou seja vírus, hackers, spam e spyware. Uma interface de utilizador comum permite a configuração e gestão de todas as componentes da solução.

A função de protecção anti-vírus inclui:

- **Análise anti-vírus do tráfego de e-mail** ao nível dos protocolos de transmissão de dados (POP3, IMAP e NNTP para e-mails de entrada e SMTP para e-mails de saída) independentemente do cliente de e-mail utilizado. O programa inclui plug-ins para os clientes de e-mail mais populares (Microsoft Office Outlook, Microsoft Outlook Express (Programa de e-mail do Windows) e o The Bat!) e suporta a desinfecção das suas bases de dados de e-mail.
- **Análise, em tempo real, do tráfego de Internet** transferido via HTTP.
- **Protecção do sistema de ficheiros**: análise anti-vírus de ficheiros individuais, directórios ou unidades. Para além disso, a aplicação pode efectuar análises anti-vírus exclusivamente para áreas críticas do sistema operativo e objectos de arranque do Microsoft Windows.
- **Protecção pró-activa**: o programa faz a monitorização constante da actividade das aplicações e processos a decorrer na memória de acesso aleatório (RAM), impedindo alterações perigosas ao sistema de ficheiros e registo e restaura o sistema após influência maliciosa.

A **Protecção contra fraude na Internet** é garantida devido à capacidade de reconhecer ataques de “phishing”, o que ajuda a prevenir fugas de dados confidenciais (primeiro de tudo, das suas passwords, números da conta bancária e cartões de crédito) e bloqueia a execução de scripts perigosos nas páginas de Internet, janelas que se abram (pop-up) e faixas publicitárias (banners). A funcionalidade **bloquear chamadas telefónicas a pagar no destino** ajuda a identificar o software que tenta usar o modem para ligação secreta não-autorizada a serviços de telefone pagos e previne essa actividade. O módulo de *Controlo de Privacidade* mantêm seguras as suas informações confidenciais em relação ao acesso e transmissão não autorizados. O *Controlo Parental* é uma componente do Kaspersky Internet Security que monitoriza o acesso dos utilizadores à Internet.

O Kaspersky Internet Security 7.0 **regista tentativas de procura de portas do computador**, que frequentemente precedem ataques de rede e defende efectivamente contra ataques típicos de hackers. O programa usa as **regras definidas como base** para controlo de todas as transacções de rede, analisando todos os **pacotes de dados de entrada e de saída**. O **Modo Furtivo** (devido à tecnologia SmartStealth™) **impede a detecção do computador a partir do exterior**. Quando muda para esse modo, o sistema bloqueia toda a actividade de rede, excepto algumas transacções permitidas por regras definidas pelo utilizador.

O programa emprega uma abordagem complexa da filtragem anti-spam de e-mails de entrada:

- Verificação de listas negras e brancas de destinatários (incluindo endereços de sites de phishing).
- Inspecção de frases no corpo da mensagem.
- Análise do texto da mensagem usando um algoritmo de auto-aprendizagem.
- Reconhecimento de spam enviado em ficheiros de imagem.

Kaspersky Anti-Virus Mobile

O Kaspersky® Anti-Virus Mobile fornece protecção anti-vírus para dispositivos móveis com os sistemas operativos Symbian OS e Microsoft Windows Mobile. O programa fornece uma protecção anti-vírus abrangente, incluindo:

- **Verificação (sob pedido)** da memória do dispositivo móvel, cartões de memória, pastas individuais ou ficheiros específicos. Se for detectado um ficheiro infectado, este é movido para a pasta da Quarentena ou é apagado.

- **Verificação em tempo real -** analisa automaticamente todos os ficheiros de entrada ou saída, assim como ficheiros quando são efectuadas tentativas para lhes aceder.
- **Protecção em relação a spam em mensagens de texto**.

Kaspersky Anti-Virus para Servidores de Ficheiros

Este pacote de software fornece protecção credível para os sistemas de ficheiros em servidores com os sistemas operativos Microsoft Windows, Novell NetWare, Linux e Samba, em relação a todo o tipo de software malicioso. O pacote inclui as seguintes aplicações da Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus para Windows Server.
- Kaspersky Anti-Virus para Linux File Server.
- Kaspersky Anti-Virus para Novell Netware.
- Kaspersky Anti-Virus para Samba Server.

Características e funcionalidade:

- *Protege os sistemas de ficheiros de servidores em tempo real*: Todos os ficheiros do servidor são analisados quando abertos ou guardados no servidor.
- *Impede surtos de vírus*.
- *Verificações sob pedido* de todo o sistema de ficheiros ou ficheiros e pastas individuais.
- *Uso de tecnologias de optimização* ao verificar objectos no sistema de ficheiros do servidor.
- *Reversão do sistema após ataques de vírus*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Monitorização do equilíbrio de carga do sistema*.
- *Criação de uma lista de processos confiáveis* cuja actividade no servidor não é sujeita ao controlo pelo pacote de software.
- *Administração remota* do pacote de software, incluindo instalação, configuração e administração centralizada.

- *Armazenamento de cópias de segurança de objectos infectados ou apagados* caso necessite de restaurá-los.
- *Colocação na quarentena* de objectos suspeitos.
- *Envio, ao administrador do sistema, de notificações sobre eventos* no funcionamento do programa.
- *Registo de relatórios detalhados*.
- *Actualização automática* das bases de dados do programa.

Kaspersky Open Space Security

O Kaspersky Open Space Security é um pacote de software com uma nova abordagem de segurança para as redes empresariais actuais de qualquer dimensão, fornecendo a protecção centralizada dos sistemas de informação e suporte para escritórios remotos e utilizadores de telemóveis.

O pacote inclui quatro programas:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

As especificidades de cada programa são apresentadas de seguida.

Kaspersky WorkSpace Security é um programa para a protecção centralizada de estações de trabalho no interior e no exterior das redes empresariais, relativamente às actuais ameaças da Internet (vírus, spyware, ataques de hacker e spam).

Características e funcionalidade:

- *Protecção abrangente em relação a vírus, spyware, ataques de hacker e spam*.
- *Defesa Pró-activa* em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Reversão para alterações maliciosas ao sistema*.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.

- *Administração remota* do pacote de software, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (*Controlo de Admissão de Rede*).
- *Verificação de tráfego de e-mail e de Internet* em tempo real.
- *Bloqueio de janelas de popup e faixas publicitárias (banner ads)* quando navega na Internet.
- *Funcionamento seguro em qualquer tipo de rede*, incluindo Wi-Fi.
- *Ferramentas de criação de disco de recuperação* que permitem restaurar o seu sistema após um surto de vírus.
- *Sistema alargado de relatórios* sobre o estado de protecção.
- *Actualizações automáticas das bases de dados*.
- *Suporte total para sistemas operativos de 64-bit*.
- *Optimização do desempenho do programa em portáteis* (Intel® Centrino® Duo technology).
- *Função de desinfecção remota* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security fornece uma protecção óptima dos recursos de informação da sua empresa em relação às actuais ameaças da Internet. O Kaspersky Business Space Security protege as estações de trabalho e servidores de ficheiros em relação a todos os tipos de vírus, Trojans e worms, impede surtos de vírus e protege a informação ao mesmo tempo que fornece acesso rápido aos recursos da rede, por parte dos utilizadores.

Características e funcionalidade:

- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Protecção das estações de trabalho e servidores de ficheiros em relação a todos os tipos de ameaças da Internet*.
- *Tecnologia iSwift para evitar a repetição da verificação de ficheiros na rede*.
- *Distribuição de carga entre os processadores do servidor*.

- *Colocação na quarentena de objectos suspeitos* de estações de trabalho.
- *Reversão para alterações maliciosas ao sistema*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Defesa Pró-activa* para estações de trabalho em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Verificação de tráfego de e-mail e de Internet* em tempo real.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Protecção enquanto utiliza redes Wi-Fi*.
- *Autodefesa* em relação a programas maliciosos.
- *Colocação na quarentena* de objectos suspeitos.
- *Actualizações automáticas das bases de dados*.

Kaspersky Enterprise Space Security

Este programa inclui componentes para proteger estações de trabalho e servidores ligados, em relação a todas as ameaças actuais da Internet. Apaga vírus de e-mails, mantendo a informação segura, ao mesmo tempo que fornece acesso seguro aos recursos da rede, por parte dos utilizadores.

Características e funcionalidade:

- *Protecção das estações de trabalho e servidores de ficheiros em relação a vírus, Trojans e worms*.
- *Protecção dos servidores de e-mail Sendmail, Qmail, Postfix e Exim*.
- *Verificação de todos os e-mails no Microsoft Exchange Server*, incluindo pastas partilhadas.
- *Processamento de e-mails, bases de dados e outros objectos para os servidores Lotus Domino*.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Impede o envio em massa de e-mails e surtos de vírus*.

- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Defesa pró-activa* para estações de trabalho, em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Funcionamento seguro ao utilizar redes Wi-Fi*.
- *Verificação de tráfego de Internet* em tempo real.
- *Reversão para alterações maliciosas ao sistema*.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.
- *Colocação na quarentena* de objectos suspeitos.
- *Sistema alargado de relatórios* sobre o estado de protecção.
- *Actualizações automáticas das bases de dados*.

Kaspersky Total Space Security

Esta solução monitoriza todos os fluxos de dados de entrada e de saída (e-mail, Internet e todas as interacções de rede). Inclui componentes para proteger estações de trabalho e dispositivos móveis, mantém a informação segura, ao mesmo tempo que fornece acesso seguro aos recursos de informação da empresa e da Internet, por parte dos utilizadores e garante comunicação segura por e-mail.

Características e funcionalidade:

- *Protecção abrangente em relação a vírus, spyware, ataques de hacker e spam* em todos os níveis da rede empresarial, desde as estações de trabalho à portas de ligação da Internet.
- *Defesa pró-activa* para estações de trabalho, em relação a novos programas maliciosos cujas assinaturas ainda não foram adicionadas à base de dados.
- *Protecção dos servidores de e-mail e servidores ligados*.

- *Verificação de tráfego de Internet* (HTTP/FTP) em tempo real, à entrada da rede local.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Bloqueio do acesso a partir de estações de trabalho infectadas*.
- *Impede surtos de vírus*.
- *Relatórios centralizados sobre o estado de protecção*.
- *Administração remota do pacote de software*, incluindo instalação, configuração e administração centralizada.
- *Suporte para Cisco® NAC* (Controlo de Admissão de Rede).
- *Suporte para servidores proxy de hardware*.
- *Filtragem do tráfego de Internet* através de uma lista confiável de servidores, tipos de objectos e grupos de utilizadores.
- *Tecnologia iSwift para evitar a repetição da verificação de ficheiros* na rede.
- *Redistribuição dinâmica de recursos* durante verificações completas do sistema.
- *Firewall Pessoal* com sistema de detecção de intrusões e avisos de ataques de rede.
- *Funcionamento seguro para utilizadores em qualquer tipo de rede*, incluindo Wi-Fi.
- *Protecção em relação a ataques de phishing e lixo electrónico*.
- *Função de desinfecção remota* (Intel® Active Management, Intel® vPro™).
- *Reversão para alterações maliciosas ao sistema*.
- *Autodefesa* em relação a programas maliciosos.
- *Suporte total para sistemas operativos de 64-bit*.
- *Actualizações automáticas das bases de dados*.

Kaspersky Security para Servidores de E-mail

Este programa serve para proteger os servidores de e-mail e servidores ligados, em relação a programas maliciosos e spam. O programa inclui aplicação para proteger todos os servidores de e-mail típicos (Microsoft Exchange, Lotus

Notes/Domino, Sendmail, Qmail, Postfix e Exim) e também lhe permite configurar uma porta de ligação dedicada para e-mail. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus para Lotus Notes/Domino.
- Kaspersky Anti-Virus para Microsoft Exchange.
- Kaspersky Anti-Virus para Linux Mail Server.

As suas características incluem:

- *Protecção credível em relação a programas maliciosos ou potencialmente perigosos*.
- *Filtragem de lixo electrónico*.
- *Verificação de e-mails de entrada e de saída e respectivos anexos*.
- *Verificação de todos os e-mails no Microsoft Exchange Server, quanto à presença de vírus*, incluindo pastas partilhadas.
- *Processa e-mails, bases de dados e outros objectos para os servidores Lotus Notes/Domino*.
- *Filtra e-mails por tipo de anexo*.
- *Coloca na quarentena* objectos suspeitos.
- *Sistema de administração fácil de utilizar* para o programa.
- *Impede surtos de vírus*.
- *Monitoriza o estado de protecção do sistema*, utilizando notificações.
- *Sistema de relatórios* sobre o funcionamento do programa.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Actualização automática das bases de dados*.

Kaspersky Security para Portas de Ligação da Internet

Este programa fornece acesso seguro à Internet para todos os funcionários de uma organização, apagando automaticamente o software malicioso e potencialmente perigoso nos dados de entrada por HTTP/FTP. A solução inclui:

- Kaspersky Administration Kit.

- Kaspersky Anti-Virus para Proxy Server.
- Kaspersky Anti-Virus para Microsoft ISA Server.
- Kaspersky Anti-Virus para Check Point FireWall-1.

As suas características incluem:

- *Protecção credível em relação a programas maliciosos ou potencialmente perigosos*.
- *Verificação de tráfego de Internet* (HTTP/FTP) em tempo real.
- *Filtragem do tráfego de Internet* através de uma lista confiável de servidores, tipos de objectos e grupos de utilizadores.
- *Coloca na quarentena* objectos suspeitos.
- *Sistema de administração fácil de utilizar*.
- *Sistema de relatórios* sobre o funcionamento do programa.
- *Suporte para servidores proxy de hardware*.
- *Escalabilidade do pacote de software* no âmbito dos recursos de sistema disponíveis.
- *Actualização automática das bases de dados*.

Kaspersky® Anti-Spam

O Kaspersky® Anti-Spam é uma solução de software pioneira que foi desenhada para ajudar organizações com redes de pequena e média dimensão na guerra contra a invasão de e-mails indesejados (spam). O produto combina a tecnologia revolucionária da análise linguística com os métodos modernos de filtragem de e-mails, incluindo as Listas Negras de DNS e características de cartas formais. A sua combinação única de serviços permite ao utilizador identificar e eliminar até 95% de tráfego indesejado.

Instalado à entrada de uma rede, onde monitoriza, em termos de spam, os fluxos de tráfego de e-mails de entrada, o Kaspersky® Anti-Spam actua como uma barreira contra os e-mails não solicitados. O produto é compatível com qualquer sistema de e-mail e pode ser instalado num servidor de e-mail já existente ou num servidor dedicado.

O elevado desempenho do Kaspersky® Anti-Spam é garantido pelas actualizações diárias da base de dados de filtragem de conteúdos, adicionando amostras fornecidas pelos especialistas laboratoriais de linguística. As bases de dados são actualizadas a cada 20 minutos.

Kaspersky Anti-Virus® para MIMESweeper

O Kaspersky® Anti-Virus para MIMESweeper fornece uma verificação, de alta velocidade, do tráfego de SMTP nos servidores que usam o Clearswift MIMEsweeper para SMTP / Clearswift MIMEsweeper para Exchange / Clearswift MIMEsweeper para Internet.

O programa é um plug-in e efectua verificações de vírus e processa, em tempo real, o tráfego de e-mails de entrada e de saída.

B.2. Contacte-nos

Se tiver quaisquer questões, comentários ou sugestões, remeta-as a um dos nossos distribuidores ou, directamente, à Kaspersky Lab. Ficaremos gratos em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com o nosso produto. Tenha a certeza de que todas as suas recomendações e sugestões serão amplamente revistas e consideradas.

Suporte técnico	Pode encontrar informação de suporte técnico em http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
Informação Geral	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APÊNDICE C. CONTRATO DE LICENÇA

Contrato de licença de utilizador final

NOTA PARA TODOS OS UTILIZADORES: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") PARA A LICENÇA DO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS WORKSTATIONS ("SOFTWARE") PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE COMPROU ESTE SOFTWARE PELA INTERNET FAZENDO CLIQUE NO BOTÃO PARA ACEITAR, VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ACEITAR E A SER PARTE DESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS SEUS TERMOS NESTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DESTE CONTRATO, E NÃO INSTALE O SOFTWARE.

SE TIVER COMPRADO ESTE SOFTWARE NUM MEIO FÍSICO, TIVER ROMPIDO O ENVELOPE DO CD VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ESTAR LIGADO A ESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DESTE CONTRATO NÃO ROMPA O ENVELOPE DO CD, DESCARREGUE, INSTALE OU USE ESTE SOFTWARE.

SEGUNDO A LEGISLAÇÃO, REFERENTE AO SOFTWARE KASPERSKY DESTINADO A UTILIZADORES INDIVIDUAIS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY PARA PDA) COMPRADO ONLINE NA PÁGINA WEB DA KASPERSKY LAB, O CLIENTE DEVE TER UM PERÍODO DE SETE DIAS ÚTEIS DESDE A ENTREGA DO PRODUTO PARA O DEVOLVER AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE ESTE SOFTWARE NÃO TENHA O SELO DESTRUÍDO.

RELATIVAMENTE AO SOFTWARE KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY PARA PDA) NÃO ADQUIRIDO ONLINE PELA INTERNET, ESTE SOFTWARE NÃO PODE SER DEVOLVIDO NEM TROCADO, EXCEPTO EM CASO DE CONSIDERAÇÕES EM CONTRÁRIO PELO PARCEIRO QUE VENDE O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO FICA ABRANGIDA PELAS CLÁUSULAS DO PARCEIRO.

O DIREITO A DEVOLUÇÃO E REEMBOLSO ABRANGE APENAS O COMPRADOR ORIGINAL.

1. *Concessão de licença*. Sujeito ao pagamento de taxas de licença aplicáveis, e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede-lhe por este meio o direito não-exclusivo e intransmissível a usar uma cópia da versão especificada do Software e a documentação acompanhante (a "Documentação") para o termo deste Contrato apenas para os fins internos de negócio.

1.1 *Utilização*. O número de computadores que o Utilizador pode proteger com o Software está especificado no Ficheiro de Chave de Licença e indicado na janela “Serviço”. O Software não pode ser utilizado para proteger redes com mais do que este número de computadores.

1.1.1 O software está "em utilização" num dispositivo cliente quando estiver carregado na memória temporária (ou seja, memória de acesso aleatório ou RAM) ou instalado na memória permanente (por exemplo, disco rígido, CD-ROM, ou outro meio de armazenamento) desse dispositivo cliente. Esta licença autoriza-o a fazer apenas as cópias de segurança necessárias do software para seu uso legal e apenas para fins de cópia de segurança, desde que todas essas cópias contenham todos os avisos proprietários do software. Deverá manter registos do número e localização de todas as cópias do software e documentação e tomar todas as precauções razoáveis para proteger o software de cópias ou utilização não-autorizadas.

1.1.2 O Software protege o computador em relação a vírus e ataques de rede cujas assinaturas estão contidas na base de dados de assinaturas de ameaças e de ataques de rede que estão disponível nos servidores de actualização da Kaspersky Lab.

1.1.3 Se vender o dispositivo cliente onde o software está instalado, deverá assegurar que todas as cópias do software foram previamente apagadas.

1.1.4 Não deve descompilar, proceder a engenharia reversa, desmontar ou reduzir de outro modo qualquer parte deste software numa forma humanamente legível nem permitir a terceiros que o façam. A interface de informação necessária para obter interoperacionalidade do software com programas de computador criados independentemente será fornecida pela Kaspersky Lab a pedido mediante pagamento dos seus custos razoáveis e despesas de obtenção e fornecimento dessa informação. Em caso de a Kaspersky Lab o notificar que não pretende tornar essa informação disponível por qualquer razão, incluindo (sem limitação) os custos, deverá ser-lhe permitido dar os passos para obter interoperacionalidade, desde que apenas proceda a engenharia reversa ou descompile o software na medida permitida por lei.

1.1.5 Não deverá executar correcções de erros, ou modificar de outro modo, adaptar, ou traduzir o software, nem criar trabalhos derivativos do software, nem permitir a terceiros copiar o software (além do aqui expressamente permitido).

1.1.6 Não deve alugar, ceder em leasing ou emprestar o software a qualquer outra pessoa, nem transferir ou sublicenciar os seus direitos de licença a qualquer pessoa.

1.1.7 A Kaspersky Lab pode pedir ao Utilizador para instalar a última versão do Software (a última versão e o último pacote de manutenção).

1.1.8 Não deve usar o software em ferramentas automáticas, semi-automáticas ou manuais concebidas para criar assinaturas de vírus, rotinas de detecção de vírus, quaisquer outros dados ou código para detecção de código malicioso ou dados.

1.1.9 Remoção de Produtos Potencialmente Nocivos. Você reconhece e concorda que, para além da detecção de software nocivo e malicioso, o Produto também pode identificar, remover e/ou desactivar produtos potencialmente nocivos, incluindo aqueles que são considerados ou classificados como Adware (software com publicidade), Riskware (software potencialmente perigoso), Pornware (software com pornografia), etc.

2. *Suporte*.

(i) A Kaspersky Lab fornecerá os serviços de suporte ("Serviços de Suporte"), tal como está definido abaixo, por um período, especificado no Ficheiro de Chave de Licença e indicado na janela "Serviço", desde o momento da activação após:

   (a) Pagamento do montante corrente de suporte à altura, e:

   (b) O serviço de suporte técnico da Kaspersky Lab também tem direito a exigir um registo adicional do Utilizador Final para efeitos de atribuição de identificador para a prestação de Serviços de Suporte.

   (c) Até à activação do Software e/ou obtenção de identificador do Utilizador Final (ID Cliente), o serviço de suporte técnico apenas presta assistência na activação do Software e no registo do Utilizador Final.

(ii) Ao preencher o formulário de subscrição dos serviços de suporte dará consentimento aos termos da política de privacidade da Kaspersky Lab, que está presente em www.kaspersky.com/privacy, e consente explicitamente com a transferência de dados de outros países fora do seu como está definido na Política de Privacidade.

(iii) Os serviços de suporte terminarão a menos que sejam renovados anualmente por pagamento do montante para suporte anual à altura e por preenchimento do formulário de subscrição dos serviços de suporte de novo.

(iv) "Serviços de suporte" significa:

- Actualizações horárias da base de dados anti-vírus;
- Actualizações da base de dados de ataques de rede;
- Actualizações da base de dados do anti-spam;

I. Actualizações livres de software, incluindo actualizações de versão;

II. Suporte técnico alargado por e-mail e linha telefónica fornecida pelo vendedor e/ou revendedor;

III. Actualizações de detecção de vírus e desinfecção durante 24 horas por dia.

(v) Os Serviços de Suporte são fornecidos apenas se e quando possuir a última versão do Software (incluindo pacotes de manutenção) instalada no seu computador, tal como está disponível no site oficial da Kaspersky Lab (www.kaspersky.com).

3. *Direitos de propriedade*. O software está protegido por leis de direito de cópia. A Kaspersky Lab e seus fornecedores detém e retêm todos os direitos, títulos e interesse pelo software, incluindo todos os direitos de autor, patentes, marcas registadas e outros direitos de propriedade intelectual nele. A sua posse, instalação, ou utilização do software não transfere qualquer título à propriedade intelectual no software para si, e não adquire quaisquer direitos ao software excepto os definidos neste Contrato.

4. *Confidencialidade*. Concorda que o software e a documentação, incluindo a concepção específica e estrutura de programas individuais e do ficheiro de identificação de licença, constituem informação confidencial exclusiva da Kaspersky Lab. Não deve revelar, fornecer, ou disponibilizar de outra forma essa informação confidencial nalguma forma a terceiros sem o consentimento prévio da Kaspersky Lab. Deverá implementar medidas razoáveis de segurança para proteger essa informação confidencial, mas sem limitação ao exposto deverá adoptar as melhores medidas para manter a segurança do código de activação.

5. *Garantia Limitada*.

(i) A Kaspersky Lab garante que pelos (6) meses desde a primeira transferência ou instalação do Software comprado num meio físico deverá operar substancialmente em consonância com a funcionalidade descrita na Documentação quando for adequadamente utilizado e do modo especificado na Documentação.

(ii) Aceitará toda a responsabilidade pela selecção deste software para obedecer aos seus requisitos. A Kaspersky Lab não garante que o software e/ou a documentação seja apropriada a esses requisitos nem que qualquer uso seja ininterrupto ou livre de erros.

(iii) A Kaspersky Lab não garante que este software identifique todos os vírus conhecidos, nem que o software não aponte eventualmente um vírus erradamente num título não infectado por esse vírus.

(iv) A Kaspersky Lab não garante que este Software forneça protecção depois da data de validade (ver section.2 (i))

(v) A sua única solução e toda a responsabilidade da Kaspersky Lab pela quebra da garantia no parágrafo (i) será opção da Kaspersky Lab, para reparar, trocar ou reembolsar o software se for relatado à Kaspersky Lab ou sua designada durante o período de garantia. Deverá fornecer toda a informação consoante o necessário para assistir o fornecedor a resolver o item defeituoso.

(vi) A garantia em (i) não se deve aplicar se você tiver (a) feito ou causado quaisquer modificações a este software sem o consentimento da Kaspersky Lab, (b) usar o software de um modo para o qual não foi destinado, ou (c) usar o software além do permitido neste Contrato.

(vii) As garantias e condições definidas neste Contrato sobrepõem-se a todas as outras condições, garantias ou outros termos respeitantes ao fornecimento ou intenção de fornecimento, falta de fornecimento ou atraso em fornecer o software ou a documentação que deveria, mas para este parágrafo (vi) tem efeito entre a Kaspersky Lab e o cliente ou seria de outro modo implicado ou incluído neste Contrato ou qualquer contrato colateral, quer por estatuto, lei comum ou de outra forma, todos aqui excluídos (incluindo, sem limitação, as condições implicadas, garantias ou outros termos como qualidade satisfatória, capacidade para o fim adequado ou como utilização de perícia razoável e cuidado).

6. *Limitação de responsabilidade*.

(i) Nada neste Contrato deverá excluir ou limitar a responsabilidade da Kaspersky Lab por (a) prejuízo de fraude, (b) morte ou acidente pessoal causado pela sua quebra de dever comum legal de cuidado ou qualquer quebra negligente de um termo deste Contrato, ou (c) qualquer outra responsabilidade que não possa ser excluída por lei.

(ii) Sujeito ao parágrafo (i) acima, o fornecedor não deverá ter nenhuma responsabilidade (se em contrato, prejuízo, restituição ou de outra forma) por qualquer dos seguintes prejuízos ou danos (se esses prejuízos ou danos foram previstos, previsíveis, conhecidos ou em contrário):

   (a) Perda de rendimento;

   (b) Perda actual ou antecipada de lucros (incluindo perda de lucros em contratos);

   (c) Perda da utilidade do dinheiro;

(d) Perda de economias antecipadas;

(e) Perda de negócio;

(f) Perda de oportunidade;

(g) Perda de valor da empresa;

(h) Perda de reputação;

(i) Perda de, danos a ou corrupção de dados, ou:

(j) Qualquer perda indirecta ou em consequência ou danos de alguma forma provocados (incluindo, para evitar dúvida, onde tal perda ou dano é do tipo especificado nos parágrafos (ii), (a) a (ii), (i).

(iii) Sujeito ao parágrafo (i), a responsabilidade da Kaspersky Lab (quer seja em contrato, prejuízo, restituição ou noutra forma) resultante de ou em ligação com o fornecimento do software não pode em caso algum exceder uma soma igual ao montante pago igualmente por si pelo Software.

7. Este Contrato contém o estipulado completo entre as partes no que respeita à matéria de assunto aqui feita e sobrepõe-se a todo e qualquer estipulado prévio, compromissos e promessas entre si e a Kaspersky Lab, quer orais ou por escrito, que foram concedidas ou podem estar implicadas por qualquer escrito ou dito em negociações entre nós ou o nosso representante antes deste Contrato, e todos os contratos prévios entre as partes relacionados com os assuntos anteriormente referidos deverão cessar para ter efeito desde a Data Efectiva.

Quando utilizar o software de demonstração, não tem direito ao Suporte Técnico especificado na Cláusula 2 deste CLUF, nem tem direito a vender a cópia que possui a outras partes.

Tem direito a utilizar o software para efeitos de demonstração pelo período de tempo especificado no ficheiro de chave de licença, a contar do momento de activação (este período pode ser visualizado na janela Serviço da Interface Gráfica do Utilizador do software).